(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
21 March 2002 (21.03.2002)

PCT

(10) International Publication Number
WO 02/23367 A1

(51) International Patent Classification[7]: G06F 15/173, 15/16

(21) International Application Number: PCT/US01/28538

(22) International Filing Date:
14 September 2001 (14.09.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/232,512 14 September 2000 (14.09.2000) US

(71) Applicant *(for all designated States except US)*: GEMPLUS [/]; Avenue du Pic de Bertagne, Parc D'Activities de Gemenos, F-13881 Gemenos Cedex (FR).

(72) Inventors; and

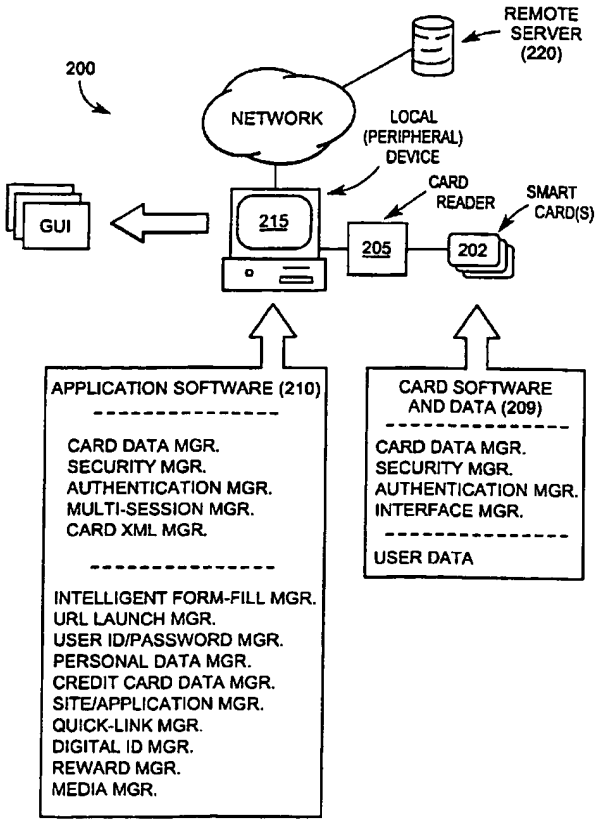
(75) Inventors/Applicants *(for US only)*: AZZOLINA, Scott, J. [US/US]; 2564 New Market Square North, Ben Salem, PA 19020 (US). MURRAY, Joseph, P. [US/US]; 49 Glen Drive, Yardley, PA 19067 (US). LANDAU, Steven, A. [US/US]; 156 Cherry Tree Lane, Cherry Hill, NJ 08002 (US). RING, John, J. [US/US]; 965 Chanticleer Mews, Cherry Hill, NJ 08003 (US). HOWARD, Thomas, D. [US/US]; 27 West Knowlton Road, Media, PA 19063 (US). LISIMAQUE, Gilles [US/US]; 1508 Blue Meadow Road, Potomac, MD 20854 (US).

(74) Agent: KRESLOFF, Mark, R.; Burns, Doane, Swecker & Mathis, L.L.P., P.O. Box 1404, Alexandria, VA 22313-1404 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH,

[Continued on next page]

(54) Title: SMART DEVICE FACILITATING COMPUTER NETWORK INTERACTION



(57) Abstract: A smart object (202), such as a smart card, a device (205) containing a smart card, or a device capable of operating in a manner that is equivalent to a smart card, is used to facilitate interaction with a computer and/or a computer based network, including, but not limited to the Internet (220). When used in conjunction with application software (210), a peripheral device (e.g., a personal computer) (215), one or more computer and/or telecommunications networks, and possibly, back-end network services, a number of features are provided, including an automatic, on-line form fill featur a user identification code (ID) and password storage and maintenance feature, a personal data storage and maintenance feature, a credit card data storage and maintenance feature, an automatic browser and URL launch feature, a favorite site/application feature, an intelligent on-line form fill feature, a digital signature capture and storage feature, a media transference management feature, a card XML feature, a personal network management and transaction feature, a quick-link feature, and an on-line reward accumulation, redemption and transfer feature.

WO 02/23367 A1

GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) **Designated States** *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

SMART DEVICE FACILITATING COMPUTER NETWORK INTERACTION

FIELD OF INVENTION

The present invention involves smart objects, for example, integrated component based end-user cards commonly known as "smart cards", or devices that contain smart objects. More specifically, the present invention involves a smart device or object that provides, among other things, a secure, personalized, portable interface that facilitates computer network interaction (e.g., intranet and/or internet interaction).

BACKGROUND

Smart cards have been in use for quite some time. In general, smart cards resemble credit cards. Unlike typical credit cards, however, smart cards contain a semiconductor chip(s) that include a built-in memory and, in most conventional smart devices, a microprocessor. The incorporation of microprocessors into smart cards has resulted in cards that are highly versatile. For instance, smart cards that contain microprocessors are capable of storing and executing programs (e.g., applets) which can, in turn, be used to provide a wide range of functionality.

Typically, systems and/or devices that employ smart cards include at least two fundamental components. First, there is the smart card itself. Second, such systems include an interface device, or card reader. The card reader is actually an input/output (i.e., read/write) device that communicates with the smart card in a secure manner in order to access the information stored therein. In one type of system, the smart card is inserted into a slot in the card reader which brings electrical contacts in the reader into engagement with mating contacts on the exterior of the smart card. The engaged contacts enable a microcontroller in the card reader to communicate with the memory and/or microprocessor in the smart card. The reader is generally connected to any one of a number of different local

or peripheral devices depending on the type of system into which the card reader is incorporated. In a security system, for example, the card reader might be connected to an electronic lock that permits a door to be opened. In a banking system, the reader could be incorporated into an automatic teller machine. Of particular relevance to the present invention, the local or peripheral device might be a personal computer, or any other like device that permits a end-user to interact with a computer network, such as the Internet, via a wireline or wireless interface. Other such devices include, but are in no way limited to kiosks, mobile telephones, laptop computers and personal digital assistants (i.e., PDAs), where the smart card may be connected thereto or contained therein.

Presently, there are several known smart card products designed to facilitate interaction with the Internet. A first example is a product called *Smart Passky*. The primary feature associated with this product is its ability to capture and store a end-user identification code (ID) and password that is used to access a particular Internet site. However, this process is not automated; it is manual. Thus, the end-user must perform several cumbersome, time consuming steps in order to capture and store a given end-user ID and password. Moreover, when the end-user attempts to log on to an Internet site, providing the corresponding end-user ID and password is also a manual process which, at best, requires the end-user to drag-and-drop the information into the appropriate location in order to gain access to the site.

A second example of a known smart card product designed to facilitate Internet usage is a product called *Pocket Server*. Pocket Server also has the ability to capture end-user ID and password information. However, it too is a manual process. Like *Smart Passky*, *Pocket Server* is unable to automatically determine when a end-user ID and password are needed to access a corresponding Internet site, and thereafter, provide the end-user ID and password without further end-user involvement.

Still another known smart card product is *Password Officer*. Password Officer is capable of storing a number of end-user passwords and log-in sequences. It is also capable of automatically providing that information to a website in order to gain access thereto. However, *Password Officer* lacks the ability to automatically and dynamically capture such information. In order to achieve this, the end-user might have to create a macro, wherein a different macro might be required in each instance.

Additionally, there are a number of non-smart card products that are designed to facilitate computer network interaction. While some of these products are also capable of storing and supplying end-user information, these non-smart card based products, in general, inherently fail to provide a number of features that smart card products are capable of providing, such as portability, personalization, and reliable end-user authentication to name just a few.

One exemplary non-smart card product is *Gator*. Though Gator is, to some extent, capable of automatically providing end-user ID and password information, as well as other information, Gator does so through a proxy technique, whereby a remote website (i.e., a proxy server) gathers the information from the end-user, and thereafter, provides the information to the website that requires the information. One significant drawback with this proxy server technique is that the end-user's personal information is transmitted over the Internet; thus, it runs the risk of being compromised.

Given the various limitations associated with smart card and non-smart card based products, and the ever increasing dependence on computer network communications, there is a strong need to simplify and automate features such as automatic end-user ID and password capture, as well as automatic form-fill, end-user authentication, personalization and portability into a single product.

SUMMARY OF THE INVENTION

The present invention is directed to a smart object, such as a smart card, a

smart device containing a smart card, or a smart device capable of operating in a manner that is equivalent to a smart card, which facilitates access to and interaction with a computer network, including, but not limited to the Internet. In general, the smart device or object is but one component in a larger system that includes application software, a local or peripheral device (e.g., a personal computer), one or more computer and/or telecommunications networks, and possibly, back-end network services.

In accordance with one exemplary configuration, the application software is stored on an executed from the peripheral device, while end-user data (e.g., personal information, end-user identification codes and passwords) is stored in the smart device or object. However, in other exemplary configurations, the application software might be stored on and executed from the smart device or object. The application software, along with the end-user data, provides the end-user with a number of unique functions, some of which are available to the end-user through a portable, personalized user interface (UI), such as a graphical user interface (GUI) which, in turn, is displayable to the end-user through the local or peripheral device. The features include, for example, a end-user identification code (ID) and password storage and maintenance feature, a personal data storage and maintenance feature, a credit card data storage and maintenance feature, an automatic browser and universal resource locator (URL) launch feature, a favorite site/application storage and maintenance feature, a digital identification capture and store feature, a personal network management and transaction feature, a quick-link feature, an on-line reward accumulation, redemption and transfer feature, a media download feature, and a card XML feature.

Another feature is the automatic, on-line form-fill feature. This feature facilitates the user's ability, for example, to complete on-line transactions or gain access to network sites, where it is first necessary to complete a corresponding on-line form. In general, the user selects one of a number of personal profiles that are stored in the memory of the smart device; one of a number of credit card

profiles stored in the memory of the smart device; and/or one of a number of user identification and password profiles stored in the memory of the smart device. The feature then automatically transfers information associated with these various "default" profiles directly to a remote entity, such as a remote service provider, which requires the completion of the on-line form.

One objective of the present invention is to simplify access, navigation and e-commerce in a computer and/or telecommunication network environment using a personalized, private and portable solution.

Another objective of the present invention is to facilitate access to an interaction with a computer and/or telecommunications network, and more particularly, sites and/or applications associated therewith.

It is another objective of the present invention to personalize and/or customize a end-user's ability to access and interact with the computer and/or telecommunications network.

It is still another objective of the present invention to provide the end-user with a personalized and/or customized access and interaction solution that is also portable.

It is yet another objective of the present invention to provide the issuer of the smart object, smart device, or smart card with the capability to control the end-user's ability to access and interact with the network.

It is another objective of the present invention to provide a substantial degree of privacy and security to protect the personal, confidential information that is stored on or in the smart object, device or card.

In accordance with a first embodiment of the present invention, the above-identified and other objectives are achieved by a computer network based system. The system includes, among other features, a first network device and a smart device that is capable of communicating with the first network device. The smart device comprises means for storing one or more data entries that represent personal information that is associated with the user of the smart device. In

addition, the system includes a second network device that is connected to the first network device by a computer network. Still further, the system includes means for analyzing one or more data requests which have been transferred from the second network device to the first network device via the computer network; means for matching each of the one or more data requests with a corresponding one of the stored data entries; and means for automatically transferring to the second network device, from the first network device, one or more data sequences, each being associated with a corresponding one of the stored data entries.

In accordance with a second embodiment of the present invention, the above-identified and other objectives are achieved by a method for completing an on-line form, where the method is employed in a system that includes a smart device, a first network device, a second network device and a computer network connecting the first network device and the second network device. The method includes, among other features, the step of storing one or more data entries in a memory associated with the smart device, where each of the one or more data entries represents information that is associated with a user of the smart device. The method further involves transferring an on-line form from the second network device to the first network device via the computer network, where the on-line form includes one or more data elements. Once the on-line form has been transferred, each of the one or more data elements are compared to one or more of the stored data entries. Then, one or more data sequences are transferred from the first network device to the second network device, where each data sequence is associated with a corresponding data entry that matches a data element.

In accordance with a third embodiment of the present invention, the above-identified and other objectives are achieved by a method for completing an on-line form, where the method is employed in a system that includes a smart device, a peripheral device and a remote network server that is connected to the peripheral device by a computer network. The method includes the step of displaying the on-

line form on a display that is associated with the peripheral device. Thereafter, a model of the on-line form is created, where the model comprises a plurality of data elements that are associated with the on-line form. The method then involves analyzing a pattern associated with each of the data elements; comparing the data pattern associated with each of the data elements to a data pattern associated with one or more data entries stored in memory on the smart device; and associating a data entry with a corresponding data element if the data pattern of the data entry matches the data pattern of the data element. A data sequence associated with the data entry is then transferred from the memory on the smart card to the model of the on-line form, if the data pattern of the data entry matches the data pattern of the data element, where the data sequence represents information associated with the user of the smart device. Finally, the on-line form is re-displayed, where the on-line form includes one or more data sequences, each being associated with a corresponding one of the plurality of data elements.

BRIEF DESCRIPTION OF THE FIGURES

The objectives and advantages of the present invention will be understood by reading the following detailed description in conjunction with the drawings, in which:

Figures 1A and 1B illustrate a conventional, personal computer system configured to operate with a smart card, and the basic structure of an exemplary smart card and card reader respectively;

Figure 2 illustrates a smart card based system in accordance with exemplary configurations of the present invention;

Figure 3 illustrates an exemplary graphical end-user interface in accordance with the present invention;

Figures 4A and 4B illustrate an exemplary text box and flowchart, respectively, associated with an automatic browser and universal resource locator feature of the present invention;

Figure 5 illustrates the exemplary graphical end-user interface in accordance with a personal website storage and maintenance feature of the present invention;

Figures 6A, 6B and 6C illustrate the exemplary graphical end-user interface, an exemplary text box, and a flowchart, respectively, associated with a end-user identification code and password storage and maintenance feature of the present invention;

Figures 7A and 7B illustrate an exemplary text box and the exemplary graphical end-user interface, respectively, associated with a personal profile storage and maintenance feature of the present invention;

Figures 8A and 8B illustrate an exemplary text box and flowchart associated with credit card storage and maintenance feature of the present invention;

Figure 9 is a flowchart associated with an intelligent form-filling feature of the present invention;

Figures 10A and 10B illustrate an exemplary end-user interface and flowchart, respectively, associated with a personal network management and transaction feature of the present invention;

Figure 11 is a flowchart associated with a digital identification capture and storage feature of the present invention; and

Figure 12 is a flow chart illustrating an on-line reward accumulation, redemption and transfer feature.

DETAILED DESCRIPTION OF THE INVENTION

To facilitate an understanding of the principles and features of the present invention, the present invention is described hereinafter in the context of a specific embodiment. In particular, reference is made to an implementation of the invention in which a smart card can be connected to a personal computer. It will be appreciated, however, that the practical applications of the invention are not

limited to this particular embodiment. Rather, the invention can be implemented in a variety of ways and employed in a variety of different systems. Of particular interest is the utilization of the present invention in connection with local or peripheral devices other than a personal computer. Such other peripheral devices might include, but are not limited to kiosks, laptops, mobile telephones, personal digital assistants (PDAs), and other devices that are capable of communicating with smart objects and other entities over computer and/or telecommunications networks.

Figure 1A is an illustration of a conventional personal computer system 100 which is configured to operate with a smart card. As is typical, the computer system might include a central processing unit (CPU) 102 and the basic input and output devices that are employed by the end-user to interact with programs being executed by the CPU 102, such as a keyboard 105 and a monitor 110. In addition, the system 100 shown in Figure 1A includes a smart card reader 115. In actuality, the card reader 115 is an input/output (I/O) device that is capable of reading data from and writing data to the smart card. In a conventional arrangement, the exchange of information between a smart card and the card reader 115 may be carried out in accordance with a standard protocol. However, the use of a card reader that does not strictly conform to published standards is certainly foreseeable. The card reader 115 may connect to the CPU 102 via a standard input/output port, such as a Universal Serial Bus (USB) port or an RS232 serial port. Alternatively, the structure of the reader 115 might be incorporated into the housing of the CPU 102 or the keyboard 105. In accordance with other alternatives, a card reader may not be required, particularly where the smart card is incorporated into a smart device, such as a mobile telephone or PDA, which communicates with the local or peripheral device, or where the smart device communicates directly with remote entities over a telecommunications network, such is the case with a web appliance, including cable set-top boxes.

Figure 1B illustrates the basic structure of an exemplary smart card 120 and card reader 115. Generally speaking, the smart card 120 is a end-user card made of plastic or other suitable material, similar to a common credit card, having a number of electrical contacts 125 on one exterior surface thereof. Embedded within the structure of the card 120 is an electronic memory 130 and, in a preferred configuration, a microprocessor 135. For ease of illustration, the memory 130 and microprocessor 135 are shown as being offset from the contacts 125. However, in practice they can be located directly beneath the contacts. The dimensions of the card 120, and the arrangement and location of the contacts 125, are generally determined by applicable standards.

The card reader 115 has a slot 140 that is appropriately dimensioned to receive the card 120. The bottom of the slot 140 has a switch 145, or other form of sensor, to detect when the card is fully inserted into the slot. The interior surface of the slot has a set of mating contacts (not shown) which engage corresponding contacts 125 on the smart card 120 when it is fully inserted. When the switch 145 detects that smart card 120 is completely inserted into the slot 140 of the card reader 115, it sends a signal which causes the card reader 115 to initiate a power-up procedure.

Figure 2 presents an overview of a smart-device based system 200. As shown, the system 200 includes, among other elements, a smart card(s) 202, a card reader 205, smart card software and data 209, application software 210, a local computer 215, herein referred to as a peripheral device (e.g., a kiosk or a personal computer), a computer or telecommunications network (e.g., a local area network, a wide area network or the Internet), and back-end services associated with a remote service provider 220. Again, it will be understood that the card reader 205 is an input/output device that is capable of both reading and writing data to and from the smart card(s) 200.

The system 200 illustrated in Figure 2 is exemplary; thus, other configurations are certainly feasible. One such alternative configuration might

incorporate the card reader 205, as stated previously, into the structure of the peripheral device 215. In another alternative configuration, the various functions associated with the card reader 205 and the smart card(s) 202 might be integrated into a portable smart device, such as a mobile telephone or a watch, where the portable smart device may communicate with the peripheral device 215 via a wireline or wireless (e.g., RF) link. In still another alternative configuration, the application software 210 may reside in the smart card(s) 202. In yet a further alternative configuration, the peripheral device 215 may take on any number of different forms, such as a fixed device (e.g., a kiosk), a desktop device (e.g., a personal computer), a transportable device (e.g., a laptop computer) or a mobile device (e.g., a PDA or mobile telephone). However, other peripheral devices are foreseeable.

The application software 210 may be pre-loaded, downloaded or installed by the end-user through a software interface. If pre-loaded, the end-user may have the ability to alter the application software. If downloaded, for example, when the smart card 202 is first inserted into the card reader, it will be understood that the network address of the application software will be stored on the smart card 202. It will also be understood that updates to the application software might be downloaded, if necessary, upon subsequent use of the smart card.

Preferably, the application software 210 comprises a number of software modules, where each module is associated with a corresponding function. The list of modules associated with application software 210 shown in Figure 2 is in no way an exhaustive list.

A first one of these software modules is the card data manager. It is responsible for manipulating (e.g., adding, deleting, editing, backing-up, restoring) the end-user data stored on the smart card 202. This module may include a number of sub-modules, each of which is used in manipulating a corresponding type of end-user data (e.g., personal data or credit card data).

A second software module is the multi-session manager. This software module provides the end-user with the ability to simultaneously execute a plurality of browser tasks and/or other applications. Thus, in accordance with the form-fill feature, the user may be capable of filling more than one on-line or web-based form at a time.

Yet another module is the smart card 202, or smart device authentication manager. Typically, authentication involves "hand shaking" between the smart card 202 and, for example, a remote server 220. In accordance with the present invention, the authentication manager is capable of recognizing an authentication challenge issued by the remote server 220, and capable of generating an appropriate response to the challenge in order to authenticate the smart card 202. In addition, this module might provide an audible or visual indication when the smart card 202 is authenticated.

The authentication process serves at least two purposes. First, it may be used for securing the smart card (i.e., the card holder), the site, or the transaction. Thus, the authentication process helps prevent unauthorized persons from accessing a site, accessing information, using applications, and engaging in unauthorized transactions. Second, the authentication process can be used by e-commerce providers to track consumer behavior for customer segmentation and targeted marketing.

In the present invention, the authentication process may employ a triple DES (i.e., Data Encryption Standard) algorithm. If so, the remote server 220, which is attempting to authenticate the end-user, generates a random number. The DES algorithm then uses the random number, plus a master key to generate a data sequence. The data sequence is then downloaded to the application software 210. The master key needed to decrypt the random number is stored on the smart card 202. Once decrypted, the random number is transmitted back to the remote server for authentication. The master key is never transmitted. Accordingly, the smart

card 202, or smart device, must be present for authentication to occur prior to accessing a site or permitting a transaction to take place.

Another module is the Security Manager. The security manager is responsible for the security process that is associated with validating the end-user when the smart card 202 is first inserted into the card reader 205, or alternatively, when the smart device undergoes a power-on process. In the present invention, the security manager may prompt the end-user to provide an identification code when the smart card 202 is first inserted into the card reader 205, or alternatively, when the smart device is first powered-on. If, for example, an incorrect code is provided a certain number of times, the security manager may lock-out the smart card 202 (i.e., disable the smart card). When the smart card 202 is removed from the card reader 205, or when the smart device is powered-down, the security manager is responsible for closing down the entire application session on the peripheral device 215. This includes destroying all objects or data created and/or stored on the peripheral device 215 during the session, thereby helping to prevent end-user information from being compromised, where end-user information might otherwise be accessible to third parties who have or might gain access to the peripheral device memory. It will be readily apparent that use of the security manager depends upon the sensitivity of the data being stored on the smart card 202, as well as issuer or end-user preference.

Still another software module is the card XML data manager. XML refers to Extendable Markup Language. It supports web-based documents, or documents that contain structured data. More particularly, XML allows a programmer/developer, for example, of smart cards, to define customized data tags and the structural relationships between them. In the present invention, end-user data stored on the smart card 202 is preferably in XML format. As one skilled in the art will readily appreciate, the card XML manager serves as an interface between the data concepts associated with the application software 210 and the data stored on the smart card 202.

The advantages associated with the card XML manager directly affect the programmer/developer of the smart card 202. For instance, the card XML data manager makes it easier for the developer to insert new data elements without having to reformat the entire smart card. Also, it provides a more efficient data storage strategy to conserve memory space. Thus, more data can be stored on a given card or smart device.

Other software modules include a URL launch manager, a user ID/password manager, a personal data manager, a credit card data manager, a site/application manager, a quick-link manager, a digital identification manager, an intelligent form-fill manager, a reward manager, and a media manager. The features associated with each of these managers are described below in greater detail.

As stated above, with reference to the exemplary configuration of Figure 2, the smart card 202 also contains software and data 209. Like the application software 210, the card software comprises a number of software modules. Generally speaking, the software modules residing on the smart card 202 are counterpart modules that correspond with one or more of the software modules that are associated with the application software 210. Thus, in addition to end-user data, the smart card 202 may contain a data manager, a security manager, and an authentication manager.

In a preferred configuration, the card software and data 209 includes an interface manager. The interface manager is responsible for generating and maintaining a user interface (UI). In the configuration illustrated in Figure 2, the UI may be a graphical user interface (GUI) which is displayable on the peripheral device 215. Moreover, the interface manager may be capable of generating the GUI in accordance with any number of different "skins" or appearances. It is through the GUI that a end-user invokes the various features associate with the present invention. The GUI is described in greater detail below.

The application software 210, along with the card software and data 209, provide the user with a number of unique features, many of which are invoked by the end-user via the GUI. Included among these features are an user ID and password storage and maintenance feature, which is controlled by the user ID/password manager; a personal data storage and maintenance feature, which is controlled by the personal data manager; a credit card data storage and maintenance feature, which is controlled by the credit card data manager; a favorite site/application storage and maintenance feature, which is controlled by the site/application manager; an automatic browser and universal resource locator (URL) launch feature, which is controlled by the URL launch manager; an intelligent form-fill feature, which is controlled by the form-fill manager; a digital identification capture and storage feature, which is controlled by the digital identification manager; a personal network management and transaction feature, which is controlled by the quick-link manager; and an on-line reward accumulation, redemption and transfer feature, which is controlled by the rewards manager. Additionally, the application software 210 facilitates certain interactions and transactions between the remote service provider 220 and the smart card 202, the results of which may be displayed to the end-user on the GUI. The GUI and each of the aforementioned features provided by the application software 210 are now described in greater detail herein below.

Figure 3 illustrates an exemplary GUI. Those skilled in the art will readily appreciate that other types of end-user interfaces may be employed depending primarily on the nature of the peripheral device 215. Moreover, the GUI illustrated in Figure 3 may take on any of a number of appearances referred to above as "skins". As shown, the GUI includes several attributes, such as a dynamic display 300, through which the end-user can view pertinent information. Other attributes include a number of functional buttons, such as the button labeled "Passwords", which relates to the user ID and password storage and maintenance feature; the button labeled "Personal", which relates to the personal data storage

and maintenance feature; the button labeled "Credit Cards", which relates to the credit card data storage and maintenance feature; the button labeled "->URL", which relates to the automatic browser and URL launch feature; the button labeled "Digital Identity", which relates to the digital identification capture and storage feature; the button labeled "Favorites", which relates to the favorite site/application feature; and the button labeled "Me!", which relates to the intelligent form-fill feature. Still other attributes include a window 305 containing a number of "quick-link" buttons (QLB), and a QLB control icon 310. The specific function of each of these attributes will become apparent from the following discussion.

In accordance with a first aspect of the present invention, the application software 210, and in particular, the URL launch manager, as well as the card software and data 209 provide the end-user with an automatic browser and URL launch feature. When the smart card 202 is first inserted into the card reader 205, or when the smart card device containing the smart card first invokes the smart card contained therein, the security manager validates the card and the application software 210 automatically launches browser software. In addition, the URL launch manager automatically initiates a log-in and authentication process with the service provider, e.g., the Internet Service provider, if doing so is necessary. The URL launch manager then causes the browser to navigate to a particular site (e.g., website) as defined by a corresponding default network address (e.g., a URL) that has been programmed into the smart card 202. Furthermore, if the site defined by the default address requires a user ID and/or password, the required user ID and/or password is automatically provided so that the end-user is automatically connected to the site without further end-user interaction.

As stated, after inserting the smart card 202, the browser automatically connects the end-user to a default address or URL. In one configuration, the default address or URL may be preset by the issuer of the smart card 202, where the issuer of the smart card may have reasons for wanting the end-user to always

be routed to this URL. In this instance, the end-user may not have the ability to alter the default URL which has been set by the issuer of the smart card.

In another configuration, the default URL may not be preset. Here, the end-user would have the ability to set and/or alter the default URL. To achieve this, the end-user would select, for example, the button labeled "->URL" on the GUI. This, in turn, causes a UI, such as the text box illustrated in Figure 4A to be displayed. Using the text box, the end-user may enter and store a desired default URL 400 (e.g., http://gemplus/gemplus/gemplus.htm).

Figure 4B illustrates an exemplary technique that might be employed by the URL launch manager to implement the automatic browser and URL launch feature. As shown in step 420, the URL launch manager monitors the card reader 205, or more particularly, the switch or sensor 145 contained therein. When the smart card 202 is inserted into the card reader 205, the switch or sensor 145 generates a signal. The generation of this signal allows the URL launch manager to detect the insertion of the smart card 202 into the card reader 205, in accordance with step 425. At this point, the security manager may validate the end-user before the default URL is actually retrieved. The URL launch manager then retrieves the default URL which is stored in memory on the smart card 202, as shown by step 430, and launches the browser as shown by step 435. This, in turn, allows the peripheral device 215 to connect to the website whose Internet address is defined by the default URL, in accordance with step 440. It will be apparent to one skilled in the art that the step of retrieving the default URL may be triggered when a smart device containing a smart card is placed into operation (i.e., powered on), rather than being triggered by the insertion of a smart card into a card reader.

Prior to establishing a connection with the site corresponding to the default URL, or prior to accessing information at the site, additional security measures may be required. This may involve a user ID code and/or password. In one instance, the URL launch feature may automatically provide a user ID and/or

password in accordance with the user ID/password feature described below, particularly where the data to be accessed is of a non-secure nature. However, if the data to be accessed is secure of user-specific, such as personal medical information or personal financial information, the URL launch manager would require manual entry of security or access code information.

In accordance with a second aspect of the present invention, the application software 210, and in particular, the site/application manager, as well as the card software and data 209 provide the end-user with a favorite site/application storage and maintenance feature. More specifically, the site/application manager stores and maintains a list of sites (e.g., websites) and/or applications which the end-user intends to access on a frequent basis. The favorite site/application storage and maintenance feature maybe end-user defined, as described above, or it may be pre-defined, wherein the end-user is unable to alter the listing of sites and/or applications. The latter case is more applicable where the smart card is being used by the issuer of the smart card as a tool to limit end-user access. This will be explained in greater detail below.

Figure 5 illustrates a GUI with an exemplary list of favorite sites and applications presented on the dynamic display 300. The end-user can display this list by selecting, for example, the button labeled "Favorites" on the GUI. Once the list is displayed, the end-user can access any one of the sites or applications by selecting the corresponding entry from the list. In addition, the end-user may be able to add a new site or application to the list or delete a site or application from the list. In adding a site or application to the list, the end-user can manually enter the new site or application pathway to the list, drag-and-drop a site or application pathway to the list (e.g., from the browser), or cut-and-paste a site or application pathway to the list.

In accordance with a third aspect of the present invention, the application software 210 and, in particular, the user ID/password manager, as well as the card software and data 209 provide a user ID and password storage and maintenance

feature. The user ID and password storage and maintenance feature is capable of automatically capturing and storing a user ID and password. It is also capable of supplying a user ID and/or password in accordance with the intelligent form-fill feature, which is described in greater detail below, when the end-user accesses the corresponding site or application that requires the user ID and/or password. Accordingly, the end-user need not manually enter this information each time the end-user accesses the site or application. Nor does the end-user have to remember the user ID and/or password associated with each and every site or application that requires this information.

One skilled in the art will readily appreciate that the user ID and password storage and maintenance feature operates in conjunction with the aforementioned favorite site/application storage and maintenance feature. Thus, for each favorite site or application that requires an user ID and/or password, the user ID/password manager stores and maintains a corresponding user ID and/or password. If and when the end-user selects one of the favorite sites or applications, the user ID/password manager is capable of automatically supplying the user ID and/or password that corresponds to the selected site or application without any further end-user interaction.

Figure 6A illustrates a GUI with an exemplary list of sites and/or applications that require a user ID and/or password presented on the dynamic display 300. The end-user can access this list by selecting, for example, the button labeled "Passwords" on the GUI. Once the list is displayed, the end-user can manually add a new user ID and/or password or manually edit an existing user ID and/or password.

The end-user can also control whether a user ID and/or password associated with a listed site or application is to be automatically supplied in accordance with the intelligent form-fill feature. For instance, the end-user may select the website "Gifts.com" from the list presented on the dynamic display 300 in Figure 6A. In doing so, a UI appears, such as the text box illustrated in Figure

6B. The text box displays the user ID and password information corresponding to "Gifts.com". Of particular interest is the small check-box labeled "Send <Enter> to linked web page or dialog box?". By selecting this option, the application software 210 is designed to automatically transfer the user ID and password to the website, as mentioned above. However, should the end-user decide not to select this option, the end-user may still transfer the user ID and password information from the smart card memory to the website using a drag-and-drop, cut-and-paste, or manual procedure.

Figure 6C illustrates a technique that might be employed by the user ID/password manager to automatically capture and transfer a user ID and/or password. First, as indicated by step 600, the end-user attempts to access a particular site, (e.g., an Internet website) or open a particular application. The user ID/password manager then determines, as shown by decision step 605, whether the site or application requires an user ID and/or password. If it is determined that a user ID and/or password are not required, in accordance with the "NO" path out of decision step 605, the process may be terminated according to step 610. However, if it is determined that a user ID and/or password are required, in accordance with the "YES" path out of decision step 605, the user ID/password manager searches the user ID and password data stored on the smart card 202 and determines whether a user ID and/or password have been stored for the site or application to which the user is seeking access, in accordance with steps 615 and 620, respectively.

If in searching the data stored on the smart card 202, the user ID/password manager identifies a user ID and/or password associated with the site or application, as shown by the "YES" path out of step 620, the user ID/password manager then determines, in accordance with decision step 625, whether the user has selected the aforementioned option that permits the user ID and/or password to be automatically transferred. If it is determined that the end-user has opted not to have this user ID and/or password automatically transferred, as shown by the

"NO" path out of decision step 625, the process may be terminated accordingly to step 630, wherein the end-user would be required to manually supply the user ID and/or password to gain access. On the other hand, if it is determined that the end-user opted to have the user ID and/or password automatically transferred, according to the "YES" path out of decision step 625, the user ID and/or password are transferred, as shown by step 635, in accordance with an intelligent form-fill feature, which is described in detail below.

If it is determined that a user ID and/or password for the site or application have not been previously stored on the smart card 202, in accordance with the "NO" path out of decision step 620, the user ID/password manager waits to see if the end-user manually enters a user ID and/or password to gain access to the site or application, as shown by decision step 640. If the end-user does not manually enter a user ID and/or password, in accordance with the "NO" path out of decision step 640, the process may be terminated per step 630. But if the end-user manually enters a user ID and/or password, in accordance with the "YES" path out of decision step 640, the user ID/password manager prompts the end-user as to whether the manually entered user ID and/or password are to be stored on the smart card 202, as shown by step 645. The user ID/password manager now waits for the end-user's response, as shown by step 650. If the end-user does not intend to save the user ID and/or password, in accordance with the "NO" path out of decision step 650, the process may be terminated, as shown by step 655. If the end-user does intend to save the user ID and/or password, in accordance with the "YES" path out of decision step 650, the application software 210 captures the user ID and/or password automatically, and stores the information on the smart card 200, as shown by step 660.

In accordance with a fourth aspect of the present invention, the application software 210, and in particular, the personal data manager, and the card software and data 209 provide the end-user with a personal data storage and maintenance feature. With this feature, the end-user may generate and maintain a number of

personal profiles, where for the purpose of the present invention, a personal profile is a record containing personal information, such as, the end-user's name, address, telephone number, age, date of birth, and e-mail address.

Figure 7A is a dialog box that contains personal information associated with an exemplary personal profile record entitled "Dad--Work". Presumably, this personal profile contains the end-user's (i.e., dad's) personal, work related information, for example, the name of his company, his company's address, his telephone number at work and FAX number. The dialog box might also be used to enter or edit data associated with a given personal profile record.

Figure 7B shows a GUI through which the end-user might access each of the different personal profiles by first selecting, for example, the button labeled "Personal". This, in turn, causes a list of the various personal profile records that the end-user has created to be presented on the dynamic display 300. Once the list of personal profile records has been displayed, the end-user can select any one in order to display the corresponding dialog box which contains the personal information associated with the selected personal profile.

The primary purpose of the personal data storage and maintenance feature is to facilitate intelligent form-fill operations. It is understood that some websites require the end-user to provide a significant amount of personal information, particularly when the end-user is accessing the website for the first time, or engaging in an on-line purchase, transaction, and/or other similar interaction. In fact, access to a site may be denied and transactions and/or interactions may be terminated if the requested information is not provided. Providing this information can be very time consuming. By storing and maintaining this information in one or more personal profile records, the information may be can transferred quickly and, in many instances, automatically.

The transfer of personal information from one or more personal profile records to an on-line form may be initiated in a number of different ways. For instance, the end-user may initiate the transfer by performing a drag-and-drop

operation. However the transfer of personal information is preferably achieved automatically through the use of the intelligent form-fill feature which is described in greater detail below.

In accordance with a fifth aspect of the present invention, the application software 210, and in particular, the credit card manager, as well as the card software and data 209 provide the end-user with a credit card data storage and maintenance feature. With this feature, the end-user may generate and maintain any number of credit card profiles, where each profile contains the information needed to pay for an on-line transaction using a corresponding credit card.

Figure 8A is a dialog box that displays the type of information that may be associated with a credit card profile for a *Visa*®Gold card. As shown, the credit card profile identifies, among other things, the credit card itself, the credit card holder's name, the credit card account number, and the credit card expiration date.

Figure 8B shows a GUI, through which the end-user might generate a new credit card profile, or access an existing credit card profile by selecting, for example, the button labeled "Credit Cards". In so doing, a list of the existing credit card profiles are presented on the dynamic display 300 as shown. Selecting one of the credit card profiles from the dynamic display 300 would, in turn, cause the corresponding credit card information to be displayed in a format such as that which is illustrated in Figure 8A.

Like the personal data storage and maintenance feature described above, the credit card data storage and maintenance feature supports the transfer of information (i.e., credit card information) between the smart card memory and a website, for example, to facilitate on-line purchases and other similar transactions. Moreover, initiating the transfer of credit card information may be accomplished through a drag-and-drop operation. However, the transfer of credit card information may be achieved automatically through the use of the intelligent form-fill feature.

As mentioned, another aspect of the present invention is the intelligent form-fill feature. This feature facilitates the end-user's ability to complete on-line forms, execute transactions, and gain access to websites and applications by analyzing and interpreting data fields associated with on-line or web-based forms. Then, based on the end-user data stored on the smart card 202, or in the smart device, this feature completes an on-line form and, thereafter, sends the data associated with the completed form directly to the source of the on-line or web-based form. For example, the data may be sent over the Internet, directly to a remote server from which the on-line or web-based form originated, without first transmitting the data to a proxy. In doing so, data security is better ensured.

In general, the intelligent form-fill feature achieves the above-identified function by providing the end-user with the option of selecting, as a default, one of the stored personal profiles, one of the stored credit card profiles, and possibly, one of the stored user ID and/or password files. The end-user may accomplish this, for example, by selecting an option on the UI that is associated with a particular personal profile, credit card profile, and user ID and/or password file. Referring back to Figure 7A, the end-user would click on the check box marked "Is this your default profile?" to select the personal profile entitled "Dad -- work" as the default. Similarly, in Figure 8A, the end-user would click on the check box marked "Is this your default card?" to select the *Visa*® Gold credit card profile as the default.

In Figure 8B, the GUI is illustrated as having a button labeled "Me!". By selecting this button, the end-user initiates the process of transferring information contained in the default profiles to an on-line form. Accordingly, the end-user need not go through the arduous process of manually entering the required information in order to gain access to a particular website, complete an on-line transaction, or execute an application.

Figure 9 illustrates a technique that might be used to implement the intelligent form-fill manager, and automatically transfer default information from

the smart card memory to an on-line form. As shown in step 900, the end-user initiates the intelligent form-fill process. The end-user may accomplish this by selecting, for example, the "Me!" button on the GUI, as shown in Figure 8B. An on-line form typically comprises a plurality of data fields. It will be understood that the data fields associated with the on-line form have been retrieved by the intelligent form-fill manager via the browser.

Once the end-user initiates the intelligent form-fill process, the intelligent form-fill manager analyzes and interprets each data field associated with the on-line form or application, as shown by step 905. Based on this analysis, the intelligent form-fill manager then generates a model of the on-line form or application, according to step 910, where the model may comprise data fields that correspond to end-user data contained in one or more of the default profiles. Thereafter, the intelligent form-fill manager employs a pattern matching process to determine, in accordance with decision step 915, whether each data field in the model corresponds with a data entry in one of the default profiles. If, in accordance with the "YES" path out of decision step 915, there is a corresponding data entry for a given data field in the model, the intelligent form-fill manager associates the data entry with that data field according to step 920. A determination is then made as to whether there are any additional data fields associated with the model that require matching, as shown by decision step 925.

If there are additional data fields that require matching, in accordance with the "YES" path out of decision step 925, the intelligent form-fill manager determines whether there is a data entry in one of the default profiles corresponding to a next data field. If the application is unable to match a given data field in the model with a corresponding data entry in one of the default profiles, in accordance with the "NO" path out of decision step 915, the intelligent form-fill manager may ignore the data field, or alternatively, prompt the end-user to manually provide the missing information, as shown by step 930.

Once the intelligent form-fill manager addresses each data field in the model, in accordance with the "NO" path out of decision step 925, the model, including all corresponding data from the one or more default profiles is reflected back to the website or application to complete the on-line form, as shown by step 935. The process is thereafter terminated in accordance with step 940.

In accordance with a preferred configuration, the intelligent form-fill manager transfers personal, ID and/or password, and/or credit card information directly to a remote entity, such as the remote service provider that is hosting the website that requires the information. The intelligent form-fill manager does not first transfer the information to a proxy server. Thus, fewer entities have access to the personal, ID and/or password and/or credit card information, thereby minimizing the potential that the information will be compromised or otherwise misused.

Further, the intelligent form-fill manager may provide a time stamp when transferring personal, ID and/or password and/or credit card information during a form-fill operation. The timestamp represents, or is used to derive, a period of time during which the transferred information is to be considered valid. After the expiration of this period of time, the remote service provider which has received the information is no longer authorized to use it. However, to ensure that the information is not used after the expiration of the time period, an agreement with the remote service provider may be required, wherein software at the remote server, for example, renders the information unusable (e.g., by scrambling or otherwise destroying the data) when the time period expires.

Still another aspect of the present invention is the quick-link feature. The quick-link feature is primarily controlled by the quick-link manager. Among other things, the quick-link feature provides the end-user with the ability to quickly and conveniently access frequently visited sites or applications. It also provides one of several ways for the issuer of the smart card to control end-user access. Preferably, the quick-link feature is implemented using a number of

quick-link buttons (QLBs) 305 which appear on the GUI as shown in Figure 3. By selecting one of the QLBs, the quick-link manager causes the browser to access the website or application associated with the selected QLB. If the website or application requires a user ID and/or password, the user ID/password manager automatically transfers the user ID and/or password, in accordance with the user ID and password storage and maintenance feature, assuming the information is stored in memory on the smart card 202.

Figure 10A illustrates an alternative UI which displays the QLBs. If this UI is displayed, the GUI shown in Figure 3 is preferably hidden from view. To invoke the alternative UI, the end-user may select a QLB control icon 310 as shown in Figure 3. A similar QLB control icon 310 appears on the alternative UI in Figure 10A, where the selection of the QLB control icon on the alternative UI causes the GUI of Figure 3 to be re-displayed.

As stated, the quick-link feature provides a convenient way for end-users to access frequently accessed sites and applications. To achieve this purpose, the software in the peripheral device and/or the smart card may permit the end-user to program each QLB so that it corresponds with a desired website or application. However, in addition to providing the end-user with a fast, convenient way to access frequently used sites and applications, the quick-link feature also allows e-commerce providers to control end-user/consumer behavior. To achieve this latter purpose, one or more QLBs may be programmed to correspond with a site or application associated with the e-commerce provider. Where the smart card is issued by or on behalf of an e-commerce provider, the quick-link buttons may be pre-set by the e-commerce provider or an issuer on behalf of the e-commerce provider. Alternatively, the end-user/consumer may have the ability to program each quick-link button from a limited list of links provided by the issuer of the smart card or one or more e-commerce providers.

Figure 10B illustrates an exemplary technique that might be employed by the quick-link manager to link the end-user with a given website or application.

Although the example illustrated in Figure 10B indicates that each QLB is associated with a website, one skilled in the art will appreciate that each QLB may, alternatively, be associated with local sites or applications as well. As shown in step 1000, a signal indicating that the end-user has selected one of the QLBs is detected. A determination is then made, in accordance with decision step 1005, whether the end-user selected the website associated with QLB-1. If the end-user selected QLB-1, in accordance with the "YES" path out of decision step 1005, the URL that corresponds with that website is loaded into the browser, as shown by step 1010. The browser then uses the URL to connect the peripheral device with the desired website. If the end-user did not select QLB-1, in accordance with the "NO" path out of decision step 1005, a determination is made as to whether the end-user selected QLB-2, as indicated by decision step 1015. It should be apparent that this process continues until a determination is made as to which QLB was selected by the end-user. After determining which QLB the end-user selected, and after loading the corresponding URL, quick-link manager terminates the process, as shown in step 1050.

In accordance with still another aspect of the present invention, the application software 210, and in particular, the digital identification manager, as well as the card software and data 209 provide a digital identification capture, storage and maintenance feature. This feature permits the end-user to load into memory on the smart card 202, data which represents the identity of the end-user. The representation may, for example, be a picture, a biometric (e.g., a fingerprint) or a signature. Thereafter, the data representing the end-user's identity is stored on the smart card 202, and it may be used for such purposes as authenticating the end-user, on-line documents and/or on-line transactions.

Capturing the data which represents the end-user's identity, and loading the data into memory on the smart card 202 may be achieved in any of a number of different ways. For instance, the data may be scanned into memory or copied into memory from an existing file.

The end-user may invoke the digital identification manager by selecting, for example, the button labeled "Digital Identity" on the GUI illustrated in Figure 3. In the event that the digital identification involves a signature, the digital identification manager may initially prompt the end-user to trace out their signature using a mouse, an electronic pen, or some other like input device. As the end-user traces their signature, the digital identification manager determines each of a number of input device positions, and therefrom, generates a sequence of data values that define the signature. The data defining the end-user's signature is then stored in memory on the smart card 202. The digital identification manager may display the end-user's signature on the peripheral device 215 as the signature is being traced by the end-user and as the corresponding data values which represent the signature are being stored. Thus, the completion of the signature trace on the peripheral device 215 coincides with the process of storing the data values in the memory on the smart card 202.

Figure 11 illustrates, in greater detail, an exemplary technique that might be employed by the digital identification manager to capture and store data values which represent the end-user's identify.

Initially, a data signal is generated from the representation of the end-user's identify, as shown in step 1100. If the representation is a signature, the data signal may be generated by having the end-user manipulate an input device, such as a trouse or light pen, as previously suggested. If the representation is a biometric or a picture, the data signal may be generated by scanning the representation. The data signal is then sampled, and the data samples are stored according to step 1105.

The data samples may initially be stored in a buffer. Thus, in accordance with the "NO" path out of decision step 1110, the digital identification manager will continue to sample and store data values until the last data sample has been stored, as shown by the "YES" path out of decision step 1110.

The data samples are then read from the buffer, as indicated by step 1115, and stored in a memory on the smart card, as shown in step 1120. If, in accordance with a preferred embodiment, the peripheral device has a display device, the data samples may be transferred thereto and the representation of the end-user's identity may be progressively displayed, per step 1125. Thus, the step of displaying the representation of the end-user's identify and storing the samples data values in memory on the smart card may occur substantially at the same time.

As shown by decision step 1130, the representation of the end-user's identify continues to be displayed, each portion at a time, and the sampled data values continue to be stored in memory on the smart card, until the last data sample has been stored and the last portion of the representation of the end-user's identify corresponding thereto has been displayed, in accordance with the "YES" path out of decision step 1130.

The various aspects of the present invention described thus far focus primarily on features that are of particular interest to the end-user of the smart card. There are, however, aspects of the present invention that are of particular interest to the issuer of the smart card. In a commercial context, for example, the issuer of the smart card may be an employer (e.g., a company), while the end-user of the smart card is an employee. In a non-commercial context, the issuer of the smart card may be a parent, whereas the end-user of the smart card is a child.

One aspect of the present invention, which may be of particular interest to the issuer of the smart card, allows the issuer to control, or more specifically, limit the ability of one or more users to access certain websites and/or applications. In the non-commercial context, a parent may wish to control or limit the ability of a child to access and interact with certain sites and/or applications. The parent may accomplish this by issuing multiple smart cards, one for each child, wherein each smart card is personalized for a corresponding child. Thus, for example, the parent may preset or pre-program each smart card so that when a child inserts his or her smart card into the card reader, a particular URL associated with an

appropriate website that has been selected by the parent for that child is automatically launched in accordance with the aforementioned automatic browser and URL launch feature. Similarly, the parent may preset or pre-program a card so that the favorite site/application list only contains sites and/or applications that are approved by the parent. The parent may also preset or pre-program the QLBs so that each corresponds with an appropriate website and/or application.

In order to achieve the above-identified purpose, the issuer (i.e., the parent) should have the ability to "lock" the browser; that is, prevent the browser from accessing sites and/or applications that are not one of those that have been preset or preprogrammed into the smart card by the parent. One way to accomplish this is to set up the browser such that it goes to a designated proxy prior to accessing a given site or application. The proxy contains a set of rules, for example, one for each child. The rules identify the sites and/or applications that are permissible for that child. Thus, if a child attempts to access a site that he or she is not authorized to access, the rules stored at the proxy will instruct the browser to deny access to the child.

In the commercial context, the issuer of the smart card may wish to similarly control or limit the ability of employees. In this context, an employer may issue multiple smart cards, one for each employee, wherein each smart card is personalized for a corresponding one of the employees. The employer can personalize each smart card by presetting or pre-programming, for example, the automatic browser and URL launch feature, the list of favorite websites and/or applications associated with the personal site/application storage and maintenance feature, and the QLBs, in much the same way as did the parent in the non-commercial context described above.

Further in accordance with this aspect of the present invention, the issuer of the smart card may preset or pre-program each smart card so that it imposes other limitations on the end-user. For example, the issuer may wish to limit the

user based on time of use, duration of use, as well as functionality within a site or application (e.g., prohibiting the use of credit cards).

Still further in accordance with this aspect of the present invention, the issuer of the smart card may issue what are herein referred to as "membership cards". When a membership card is placed into operation or inserted into a card reader, the membership card permits the end-user to access a private site. Anyone attempting to access the site without a card would be denied such access.

There are several ways to implement membership cards. First, the card may be pre-loaded with the corresponding URL, which is transparent to the end-user. When the card is inserted into the card reader, the URL launch manager initiates the browser which then connects the end-user to the private site. Login and authentication might be unnecessary, and the card might not cause a GUI to be displayed. Second, the card maybe pre-loaded with the corresponding URL and login sequence, where the URL and login sequence is transparent to the end-user. In this case, authentication might not be necessary, and once again, the card might not cause a GUI to be displayed. Third, the card maybe pre-loaded with the corresponding URL and login sequence, as well as any keys needed for authentication. However, the card would, once again, not cause a GUI to be displayed. Fourth, the card maybe pre-loaded as described above with respect to the first implementation, but for the fact that the card contains multiple URLs, rather than one URL. Here, the card would likely cause a GUI to be displayed, where the GUI includes graphical buttons, each corresponding to one of the multiple URLs. Fifth, the card may be pre-loaded with multiple URLs as described above in the fourth implementation. However, in this implementation, the card would also be pre-loaded with login sequences as required for one or more of the multiple URLs. Sixth, the card may be pre-loaded with multiple URLs and login sequences as described above in the fifth implementation. In this implementation, the card is also pre-loaded with any keys that are needed to

support authentication. Table I summaries the six exemplary membership card implementations described above.

	MEMBERSHIP CARD IMPLEMENTATIONS			
	URL	GUI	LOGIN	AUTHENTICATION
Implementation 1	1	No	No	No
Implementation 2	1	No	Yes	No
Implementation 3	1	No	Yes	Yes
Implementation 4	Multiple	Yes	No	No
Implementation 5	Multiple	Yes	Yes	No
Implementation 6	Multiple	Yes	Yes	Yes

TABLE 1

There are also aspects of the present invention that are of particular interest to entities other than the end-user and the issuer of the smart card. These aspects, in general, involve features that enable or support transactions and/or interactions over the Internet between the end-user and one or more specific e-commerce providers.

One such aspect involves a personal network management and transaction feature. In accordance with this feature, URL information may be pre-loaded into the smart card by an e-commerce provider or on behalf of one or more e-commerce sponsors. For example, the issuer of the smart card might lease or sell a QLB to a sponsor -- the sponsor being an e-commerce provider. The appearance of the QLB on the GUI might even reflect, by way of a logo, the corresponding sponsor. Selecting the QLB might, as previously explained, cause the browser to launch a URL associated with the sponsor, or initiate a particular on-line transaction with the sponsor.

In addition to pre-loading sponsor information, a QLB might be re-programmed automatically by downloading new or updated information, such as a new sponsor name, a new logo or new URL information. Re-programming may

be initiated as a result of an event (e.g., extending a lease to a new sponsor), an action, or simply the elapse of a particular period of time.

In contrast to pre-loading e-commerce sponsor information into the smart card, the end-user may have the option to select certain sponsors from amongst a list that is provided by the issuer of the smart card. In this instance, the end-user preferably has the ability to modify or alter the information from time to time.

Further in accordance with the personal network management and transaction feature, the smart card may be used to capture specific information. For instance, consumer transaction information (e.g., purchase order confirmation information) and/or information relating to e-commerce provider sites.

Another aspect involves an on-line reward accumulation, redemption and transfer feature. This feature is primarily handled by the rewards manager. In accordance with this feature, an end-user/consumer may earn on-line rewards for taking certain action(s) with the smart card, as explained in more detail below. From the perspective of the issuer of the smart card and/or the e-commerce provider, the on-line rewards serve as an incentive (i.e., encourage) end-user/consumers to take these actions. Rewards may take the form of tokens, points, coupons, discounts, tickets, sweepstake entries, access rights/privileges, special messages/offers (e.g., displayed on the GUI), and/or free products.

The end-user/consumer may earn rewards by using the smart card 202 in any one of a number of prescribed ways. For example, the end-user/consumer may earn rewards by using the smart card 202 for the first time (e.g., by inserting the smart card into the card reader 205 and connecting to a particular website associated with the e-commerce provider offering the reward). The reward may be earned when the end-user actually logs into the site, becoming a member (e.g., by registering with the site) or simply visiting the site. Downloading information from the site onto the smart card 202, or any other location, conducting an on-line transaction (e.g., making an on-line purchase), or filling out an on-line form are additional actions that might be the basis for extending rewards to an end-

user/consumer. Rewards may also be based on the number of times the end-user has engaged in a particular activity (e.g., the frequency with which the end-user visits a given site), how recently the end-user has engaged in the activity, or, in the case of on-line purchases, how much the end-user has purchased. It will be understood, however, that the criteria set forth above is exemplary. It is foreseeable to rely on other criteria or combinations of criteria as a basis for extending on-line rewards.

The on-line reward accumulation, redemption and transfer feature may rely on the aforementioned authentication process. For example, the authentication process may be utilized by the site to authenticate the card. In so doing, the issuer of the smart card or the e-commerce provider can control the distribution of rewards and, as explained below, use this feature to track end-user/consumer behavior. Authentication of the end-user, in addition to authentication of the smart card, may or may not be desired.

Aside from earning rewards, the end-user consumer may accumulate, redeem and transfer rewards. With regard to reward accumulation, rewards may be stored in a memory on the smart card 202. Alternatively, the smart card 202 may facilitate the process of earning rewards, though the rewards may be stored in a memory associated with the peripheral device 215. Preferably, rewards may be transferred; for example, from one smart card to another. With regard to redemption, an end-user/consumer may, preferably, redeem rewards on-line or off-line. On-line redemption may involve exchanging, over the internet, a number of accumulated reward tokens for a product or service. Off-line redemption, on the other hand, may involve exchanging a number of reward tokens at a physical store, kiosk or point-of-sale.

Figure 12 summarizes the on-line reward accumulation, redemption and transfer feature. As shown by step 1205, rewards are provided based on the end-user taking some action with the smart card. This action may involve inserting the card into the card reader; visiting a particular website by selecting a corresponding

entry from the list of stored sites and/or applications illustrated in Figure 5 or by selecting a corresponding QLB; or involve any of a number of end-user actions or combinations therefor. Preferably, there is an authentication of the smart card, as illustrated in step 1210. Then, in accordance with step 1215, the end-user obtains a reward for taking the aforementioned action(s). From the perspective of the end-user, the rewards may be accumulated, transferred and, because there is value associated with rewards, redeemed for products and/or services. From the perspective of the issuer of the smart card and/or e-commerce provider, rewards may be used to influence end-user behavior (e.g., to provide an incentive for the end-user to continue taking action), and to track end-user behavior for marketing purposes.

Still another aspect involves downloading media from a website to the end-user, where the smart card, or smart device, is employed to manage the transference of the media content, and in particular the costs associated with the transaction. This feature might also involve a card authentication process, as described above, to ensure that the end-user is entitled to receive such information.

As described above, there are several aspects associated with the present invention which provide a number of features and advantages over other smart card and non-smart card based Internet solutions. Among the several features and advantages of particular interest to end-users are the ability to automatically launch a desired URL upon insertion of the smart card into the card reader, the ability to automatically provide user ID and password information to certain websites, and the ability to provide intelligent form-fill operations. Other features and advantages of particular interest to the issuer of smart cards is the ability to issue multiple, personalized smart cards so as to individually control Internet usage of one or more end-users. Finally, as the present invention involves a smart card based solution, it provides portability, personalization, privacy and security.

The present invention has now been described in accordance with several exemplary aspects and embodiments, which are intended to be illustrative rather

than restrictive. Thus, the present invention is capable of many variations in detailed implementation, which may be derived from the description contained herein by a person or ordinary skill in the art. All such variations are considered to be within the scope and spirit of the present invention as defined by the following claims.

WHAT IS CLAIMED IS:

1. A computer network based system comprising:

a first network device;

a second network device connected to said first network device by a computer network;

a smart device in communication with said first network device, said smart device comprising means for storing one or more data entries representing information associated with a user of said smart device;

means for transferring one or more data requests from said second network device to said first network device;

means for analyzing the one or more data requests;

means for matching each of the one or more data requests with a corresponding one of the stored data entries; and

means for automatically transferring to said second network device, a data sequence associated with each data entry that matches a corresponding data request.

2. The system of claim 1, wherein said smart device is a smart card comprising a memory, and wherein each of the one or more data sequences are stored as a data entry in said memory.

3. The system of claim 2, wherein said first network device comprises:

a smart card reader adapted to physically receive said smart card.

4. The system of claim 1, wherein said smart device comprises:

a smart card that contains a memory, and wherein each of the one or more data sequences are stored as a data entry in said memory.

5. The system of claim 1 comprising:

a wireless communications link between said first network device and said smart device.

6. The system of claim 1 comprising:

a wired communications link between said first network device and said smart card.

7. The system of claim 1, wherein said first network device is a personal computer.

8. The system of claim 1, wherein said first network device is a portable device.

9. The system of claim 8, wherein said first network device is a personal digital assistant.

10. The system of claim 8, wherein said first network device is a mobile telephone.

11. The system of claim 8, wherein said first network device is a portable computer.

12. The system of claim 1, wherein said smart device is a portable device.

13. The system of claim 12, wherein said smart device is a mobile telephone.

14. The system of claim 12, wherein said smart device is a personal digital assistant.

15. The system of claim 12, wherein said smart device is a portable computer.

16. The system of claim 1, wherein said smart device is a web appliance.

17. The system of claim 16, wherein the smart device is a cable set-type box.

18. The system of claim 1, wherein each of the one or more data requests corresponds to a data element associated with an on-line form.

19 The system of claim 18, wherein said first network device comprises:

means for displaying the on-line form.

20. In a system that includes a smart device in communication with a first network device, a second network device and a computer network connecting said first network device and said second network device, a method for completing an on-line form comprising the steps of:

storing one or more data entries in a memory associated with the smart device, wherein each data entry represents information associated with a user of the smart device;

transferring a number of data elements associated with an on-line form from the second network device to the first network device via the computer network;

comparing the one or more data elements to one or more of the data entries; and

transferring, to the second network device, one or more data sequences, where each data sequence is associated with a corresponding data entry that matches a data element.

21. The method of claim 20 further comprising the step of:

creating a model of the on-line form based on the data elements associated with the on-line form.

22. The method of claim 21 further comprising the step of:

associating a data sequence with a data element in the model of the on-line form if it is determined that the data entry corresponding to the data sequence matches that data element.

23. The method of claim 22 further comprising the step of:

transferring the model of the on-line form, including the one or more data elements and one or more corresponding data sequences from the first network device to the second network device via the computer network.

24. The method of claim 23 further comprising the step of:

executing an application at the second network device in response to the second network device receiving the on-line form, including the one or more data elements and the one or more data sequences.

25. The method of claim 23 further comprising the step of:

granting the user of the smart device access to a site associated with the second network device in response to the second network device receiving the on-line form, including the one or more data elements and the one or more data sequences.

26. The method of claim 23 further comprising the step of:

completing an electronic transaction in response to the second network device receiving the on-line form, including the one or more data elements and the one or more data sequences.

27. The method of claim 20 further comprising the step of:

creating a data profile, where a number of the data entries are associated with the data profile.

28. The method of claim 27, wherein the data entries associated with the data profile relate to personal information.

29. The method of claim 27, wherein the data entries associated with the data profile relate to credit card information.

30. The method of claim 27, wherein the data entries associated with the data profile relate to an identification code or password.

31. The method of claim 20 further comprising the step of:

prompting the user to manually enter a data sequence for a given data element, if it is determined that there is no data entry which matches that data element.

32. The method of claim 20, wherein said step of determining whether each of the one or more data elements matches a corresponding data entry comprises the step of:

determining whether a data element matches a corresponding data entry in accordance with a pattern matching technique.

33. The method of claim 20, wherein the smart device comprises a smart card.

34. The method of claim 20, wherein the smart device is a smart card.

35. In a system that includes a smart device, a peripheral device and a remote network server that is connected to the peripheral device by a computer network, a method for completing an on-line form comprising the steps of:

displaying the on-line form on a display that is associated with the peripheral device;

creating a model of the on-line form, wherein the model comprises a plurality of data elements associated with the on-line form;

analyzing a pattern associated with each of the data elements;

comparing the data pattern associated with each of the data elements to a data pattern associated with one or more data entries stored in memory on the smart device;

associating a data entry with a corresponding data element if the data pattern of the data entry matches the data pattern of the data element;

transferring a data sequence associated with the data entry, from the memory on the smart card to the model of the on-line form, if the data pattern of the data entry matches the data pattern of the data element, wherein the data sequence represents information associated with the user of the smart device; and

redisplaying the on-line form, wherein the on-line form includes one or more data sequences, each being associated with a corresponding one of the plurality of data elements.

36. The method of claim 35 further comprising the step of:

creating a data profile, wherein the data profile comprises a number of the data entries stored in memory on the smart device.

37. The method of claim 36, wherein each of the data entries associated with the data profile relate to personal information.

38. The method of claim 36, wherein each of the data entries associated with the data profile relate to credit card information.

39. The method of claim 35 further comprising the step of:

transferring the model of the on-line form, including one or more data sequences, from the peripheral device to the server over the computer network.

40. The method of claim 39 further comprising the step of:

executing an application at the server in response tothe server receiving the model of the on-line form, including the one or more data sequences.

41. The method of claim 39 further comprising the step of:

completing an on-line transaction in response to the server receiving the model of the on-line form, including the one or more data sequences.

42. The method of claim 39 further comprising the step of:

granting the user access to a computer network site that is associated with the server in response to the server receiving the model of the on-line form, including the one or more data sequences.

43. The method of claim 35, wherein the smart device comprises a smart card.

44. The method of claim 35, wherein the smart device is a smart card, and wherein the one or more data entries, and the data sequences associated with each of the one or more data entries are stored in memory on the smart card.

45. A system for completing an on-line form comprising:

a smart device;

a peripheral device;

a remote network server connected to said peripheral device by a computer network;

means for displaying the on-line form on a display that is associated with the peripheral device;

means for creating a model of the on-line form, wherein the model comprises a plurality of data elements associated with the on-line form;

means for analyzing a pattern associated with each of the data elements;

means for comparing the data pattern associated with each of the data elements to a data pattern associated with one or more data entries stored in memory on the smart device;

means for associated a data entry with a corresponding data element if the data pattern of the data entry matches the data pattern of the data element;

means for transferring a data sequence associated with the data entry, from the memory on the smart card to the model of the on-line form, if the data pattern of the data entry matches the data pattern of the data element, wherein the data sequences represents the information associated with the user of the smart device; and

means for redisplaying the on-line form, wherein the on-line form includes one or more data sequences, each being associated with a corresponding one of the plurality of data elements.

46. The system of claim 45 further comprising:

means for creating a data profile, wherein the data profile comprises a number of data entry stored on the smart device.

47. The system of claim 46, wherein each of the data entries associated with the data profile relate to personal information.

48. The system of claim 46, wherein each of the data entries associated with the data profile relate to credit card information.

49. The system of claim 46, wherein each of the data entries associated with the data profile relate to an identification code or password.

50. The system of claim 45 further comprising:

means for transferring the model of the on-line form, including one or more data sequences, from the peripheral device to the server over the computer network.

51. A method of accessing a network site associated with a computer network, said method comprising the steps of:

determining whether an access code is required to access the network site;

electronically searching a list of access codes stored in a memory that is associated with a smart device, wherein the electronic search is automatically triggered upon a determination that an access code is required to access the network site;

electronically identifying, from amongst the list of access codes, an access code corresponding with the network site;

transferring the identified access code to the network site via the computer network; and

accessing the site after transferring the access code.

52. A method for connecting a user to a computer network site comprising the steps of:

activating a smart card;

launching a network browser in response to the activation of the smart card; and

connecting the user to the computer network site using the network browser and a network address associated with the computer network site, wherein the network address is stored in a memory on the smart card.

53. In a smart card based system that includes a smart card, a first network device an input/output device that transmits information between the smart card and the first network device, a method for controlling the ability of an end-user of the smart card to access a computer network, said method comprising the steps of:

identifying a computer network site for the end-user of the smart card;

storing a network address in a memory on the smart card, wherein the network address corresponds with the identified network site; and

limiting end-user access to the computer network in accordance with the identified network site.

54. In a smart card based system that includes a smart card, a first network device an input/output device that transmits information between the smart card and the first network device, a method for controlling the ability of an end-user of the smart card to access a computer network through the first network device, said method comprising the steps of:

defining a computer network access time limit for the end-user of the smart card:

storing a value in a memory on the smart card, said value representing the computer network access time limit; and

limiting the end-user's ability to access the computer network in accordance with the value that has been stored in the memory on the smart card.

55. In a smart card based system that includes a smart card, a first network device an input/output device that transmits information between the smart card and the first network device, a method for controlling the ability of an end-user of

the smart card to access a computer network through the first network device, said method comprising the steps of:

identifying a control factor which relates to the end-user's ability to functionally interact with a computer network site;

storing the control factor in a memory on the smart card; and

limiting the user's ability to interact with the network site, in accordance with the control factor that has been stored in memory on the smart card.

56. In a smart card based system, a method comprising the steps of:

storing information on a smart card;

generating a user interface which includes a user-selectable option, wherein the user-selectable option is associated with a sponsor;

selecting the user-selectable option; and

accessing a network site associated with the sponsor based on the information stored on the smart card as a result of the selection of the user-selectable option.

57. A method of rewarding an end-user for using a smart card to interact with a network site, said method comprising the steps of:

detecting the end-user's use of the smart card to interact with the network site;

conveying a redeemable reward to the end-user in response to said use of the smart card to interact with the network site; and

storing the redeemable reward.

58. A smart card based system comprising:

a smart card containing a memory in which data is stored in Extendable Mark-up Language (XML);

a smart card input/output device having means for receiving said smart card and means for reading data from and writing data to said smart card; and

a peripheral device in communication with said smart card input/output device, said peripheral device comprising an XML smart card manager which servers as an interface between application software being executed by said peripheral device and data which is stored in XML format on the smart card,

wherein said XML smart card manager comprises means for programming the smart card in XML format through said smart card input/output device.

59. In a smart device based system that includes a peripheral device and a smart device, a method comprising the steps of:

reading a sequence of data samples which are associated with a representation of an end-user's identity;

storing the data samples in a memory that is associated with the smart device; and

employing the data samples for authentication purposes.

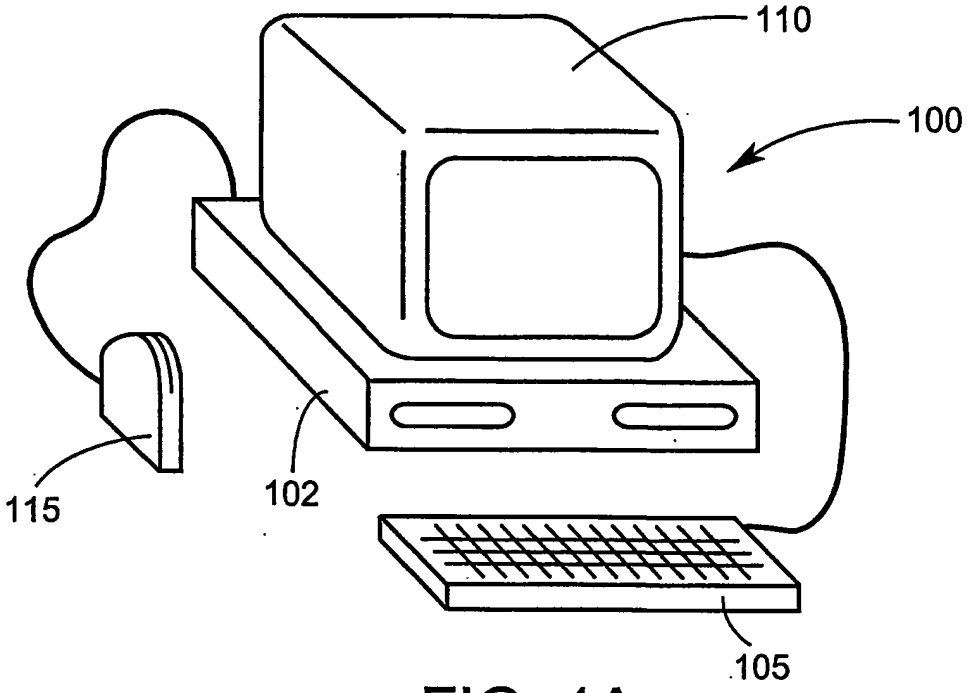


FIG. 1A

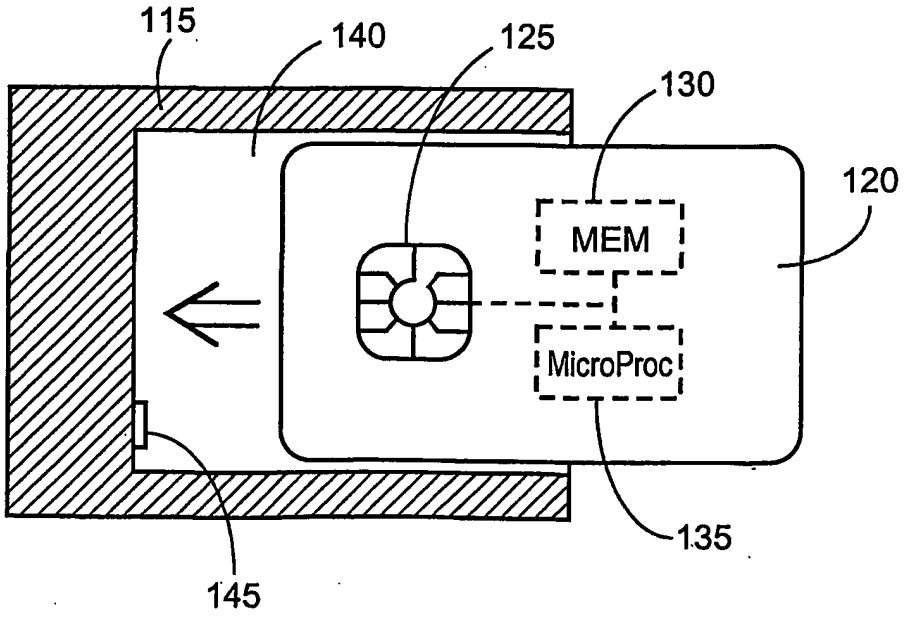


FIG. 1B

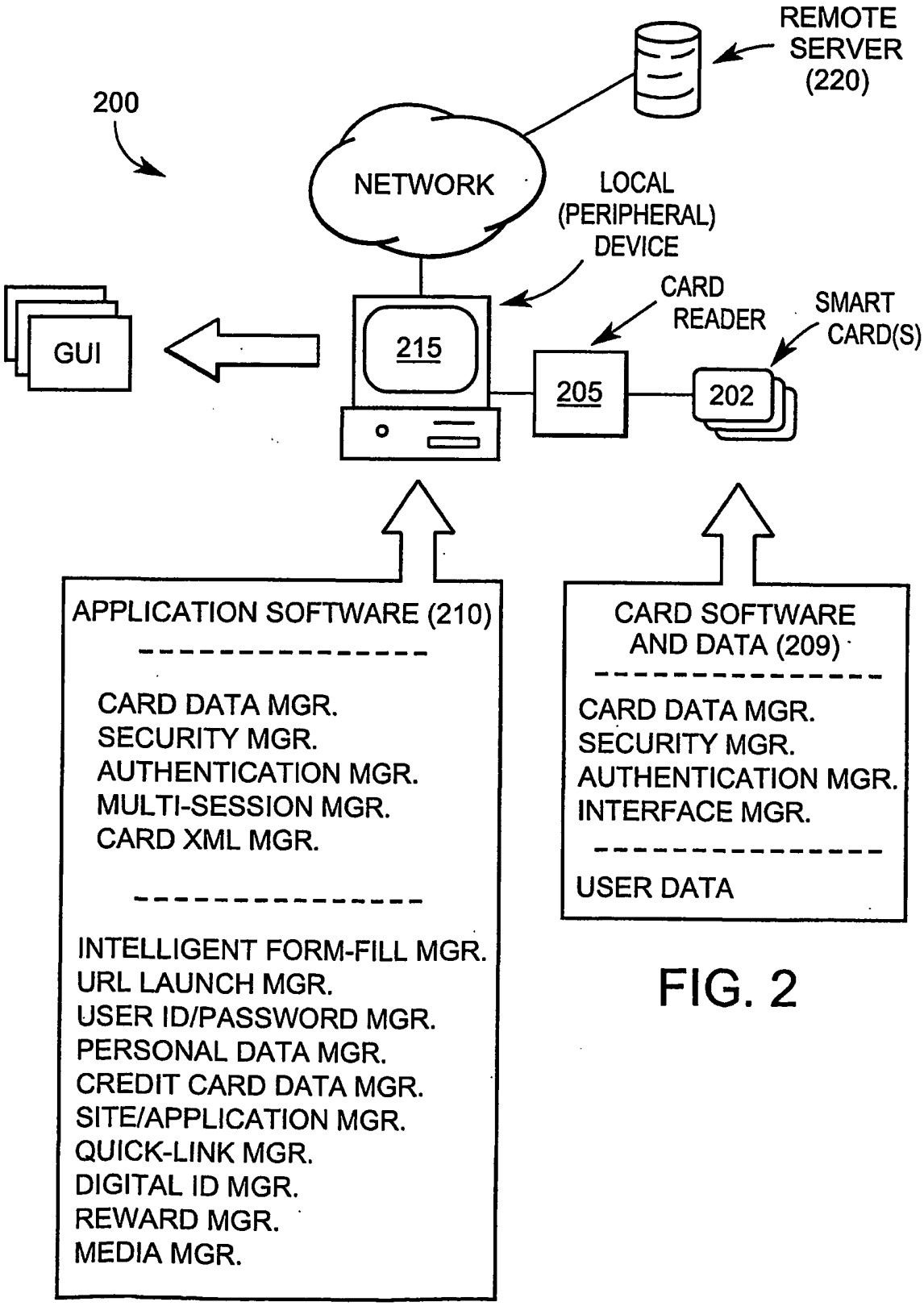

REMOTE SERVER (220)
200
NETWORK
LOCAL (PERIPHERAL) DEVICE
CARD READER
SMART CARD(S)
GUI
215
205
202
APPLICATION SOFTWARE (210)
CARD DATA MGR.
SECURITY MGR.
AUTHENTICATION MGR.
MULTI-SESSION MGR.
CARD XML MGR.
INTELLIGENT FORM-FILL MGR.
URL LAUNCH MGR.
USER ID/PASSWORD MGR.
PERSONAL DATA MGR.
CREDIT CARD DATA MGR.
SITE/APPLICATION MGR.
QUICK-LINK MGR.
DIGITAL ID MGR.
REWARD MGR.
MEDIA MGR.
CARD SOFTWARE AND DATA (209)
CARD DATA MGR.
SECURITY MGR.
AUTHENTICATION MGR.
INTERFACE MGR.
USER DATA

FIG. 2

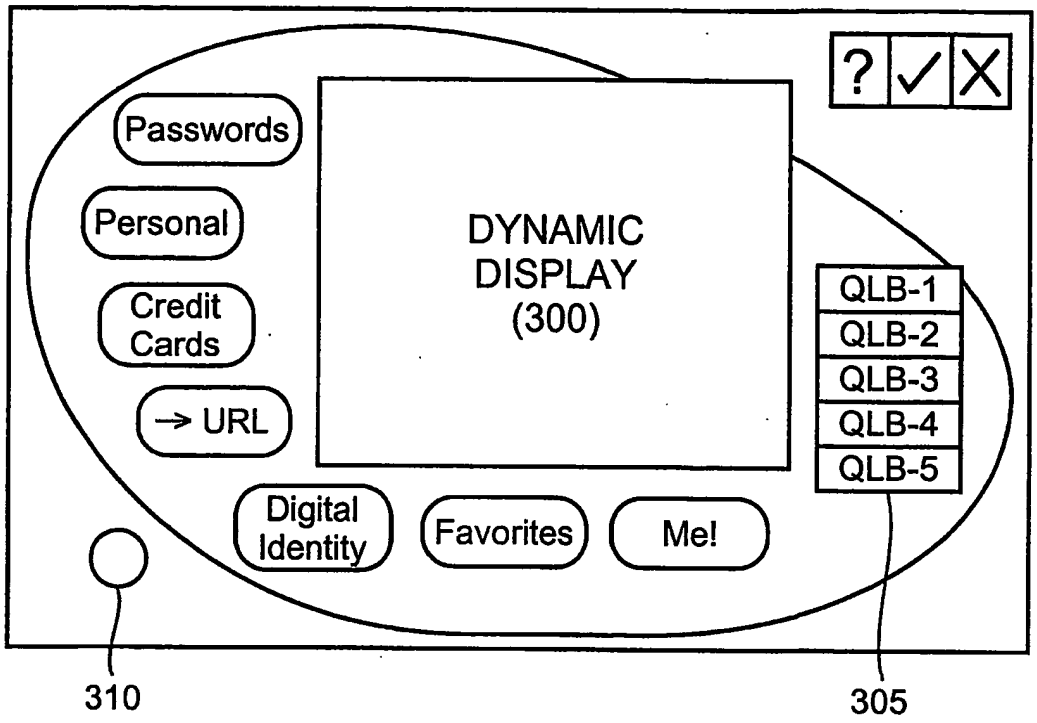

?
Passwords
Personal
Credit Cards
→ URL
DYNAMIC DISPLAY (300)
QLB-1
QLB-2
QLB-3
QLB-4
QLB-5
Digital Identity
Favorites
Me!
310
305

FIG. 3

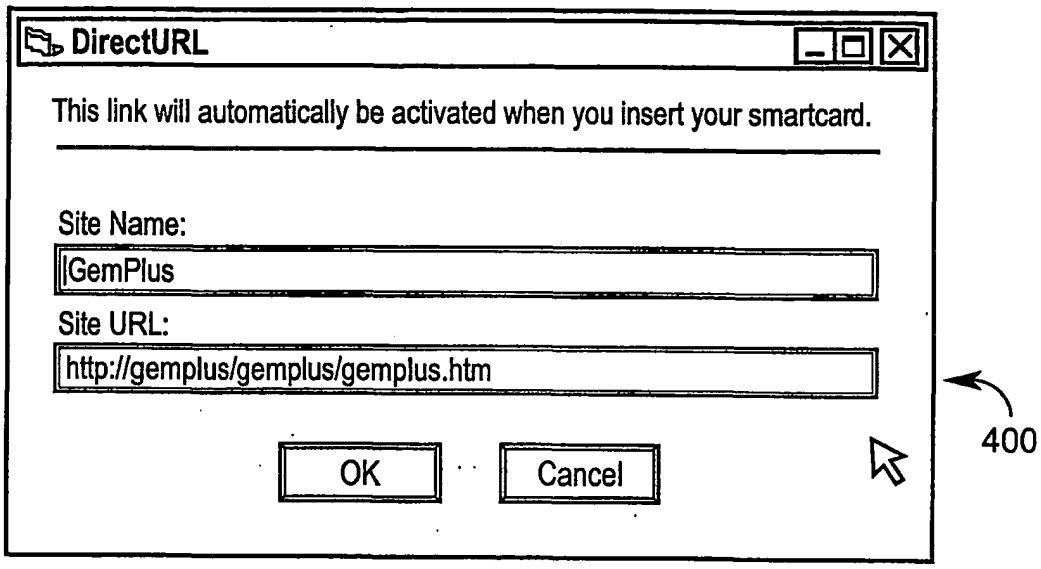

DirectURL
This link will automatically be activated when you insert your smartcard.
Site Name:
GemPlus
Site URL:
http://gemplus/gemplus/gemplus.htm
OK
Cancel
400

FIG. 4A

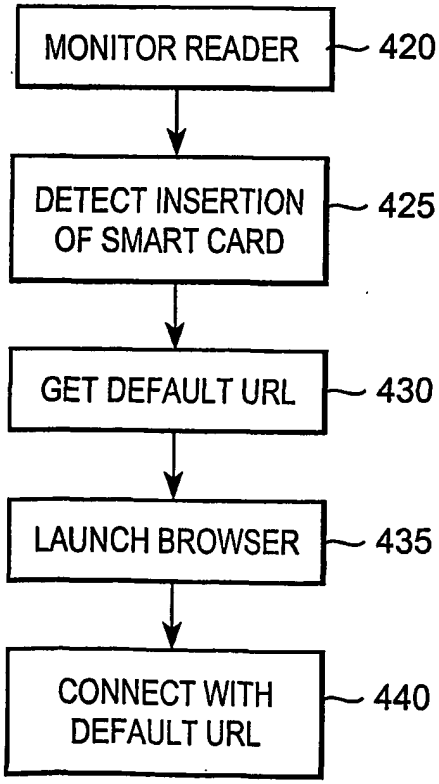

MONITOR READER
420
DETECT INSERTION OF SMART CARD
425
GET DEFAULT URL
430
LAUNCH BROWSER
435
CONNECT WITH DEFAULT URL
440

FIG. 4B

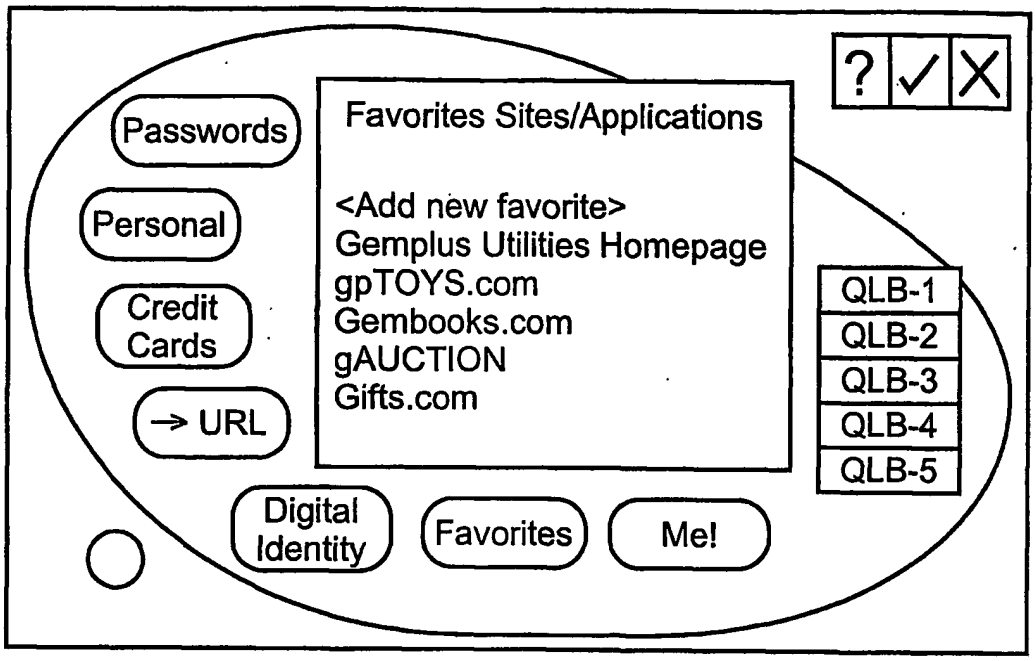

?
Passwords
Personal
Credit Cards
→ URL
Favorites Sites/Applications
<Add new favorite>
Gemplus Utilities Homepage
gpTOYS.com
Gembooks.com
gAUCTION
Gifts.com
QLB-1
QLB-2
QLB-3
QLB-4
QLB-5
Digital Identity
Favorites
Me!

FIG. 5

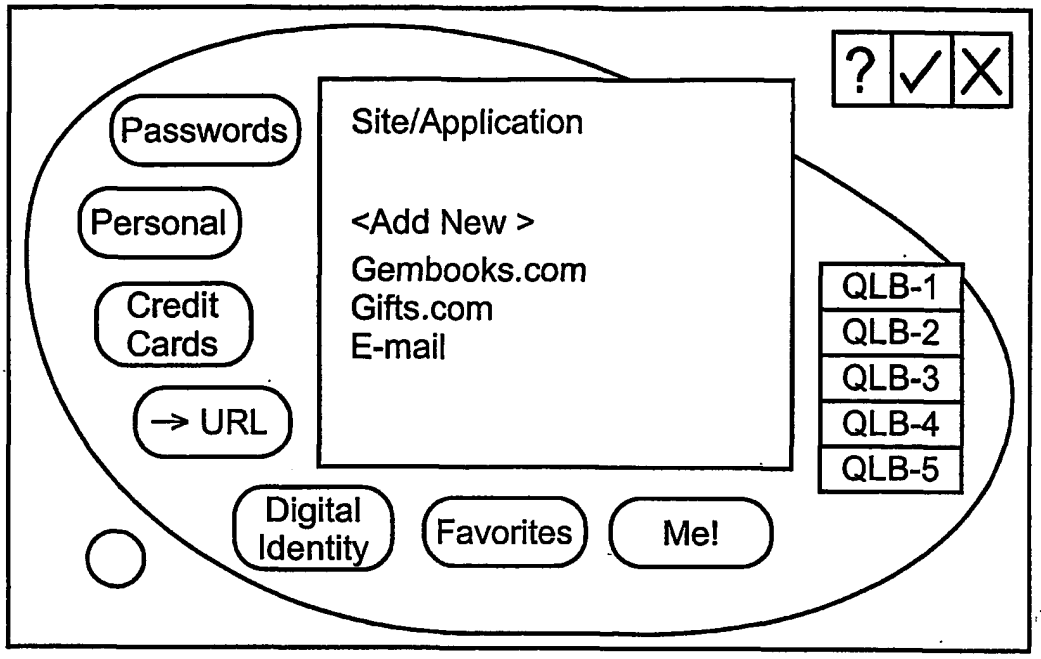

?
Passwords
Site/Application
Personal
<Add New >
Gembooks.com
Gifts.com
E-mail
Credit Cards
QLB-1
QLB-2
QLB-3
QLB-4
QLB-5
→ URL
Digital Identity
Favorites
Me!

FIG. 6A

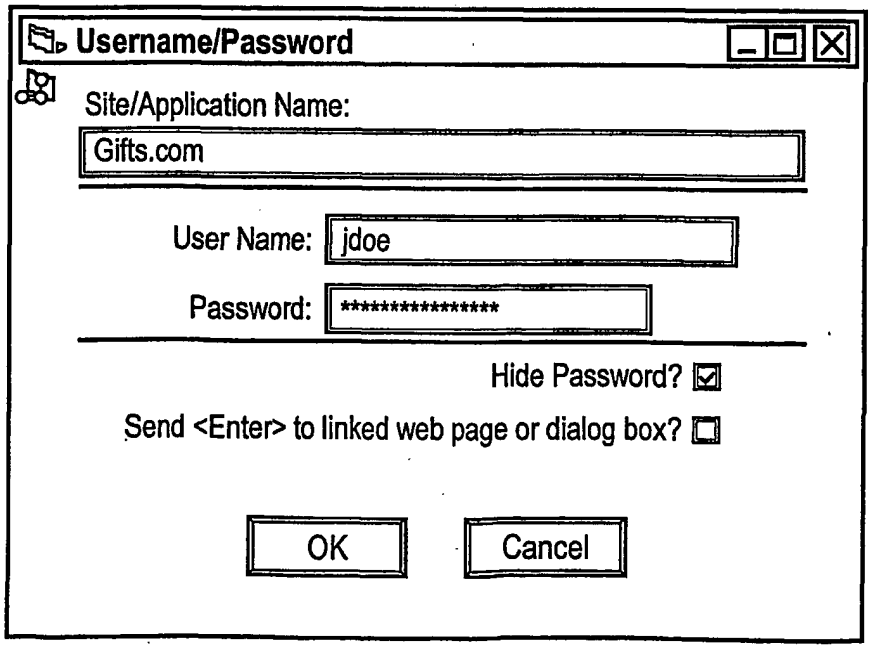

Username/Password
Site/Application Name:
Gifts.com
User Name:
jdoe
Password:
Hide Password?
Send <Enter> to linked web page or dialog box?
OK
Cancel

FIG. 6B

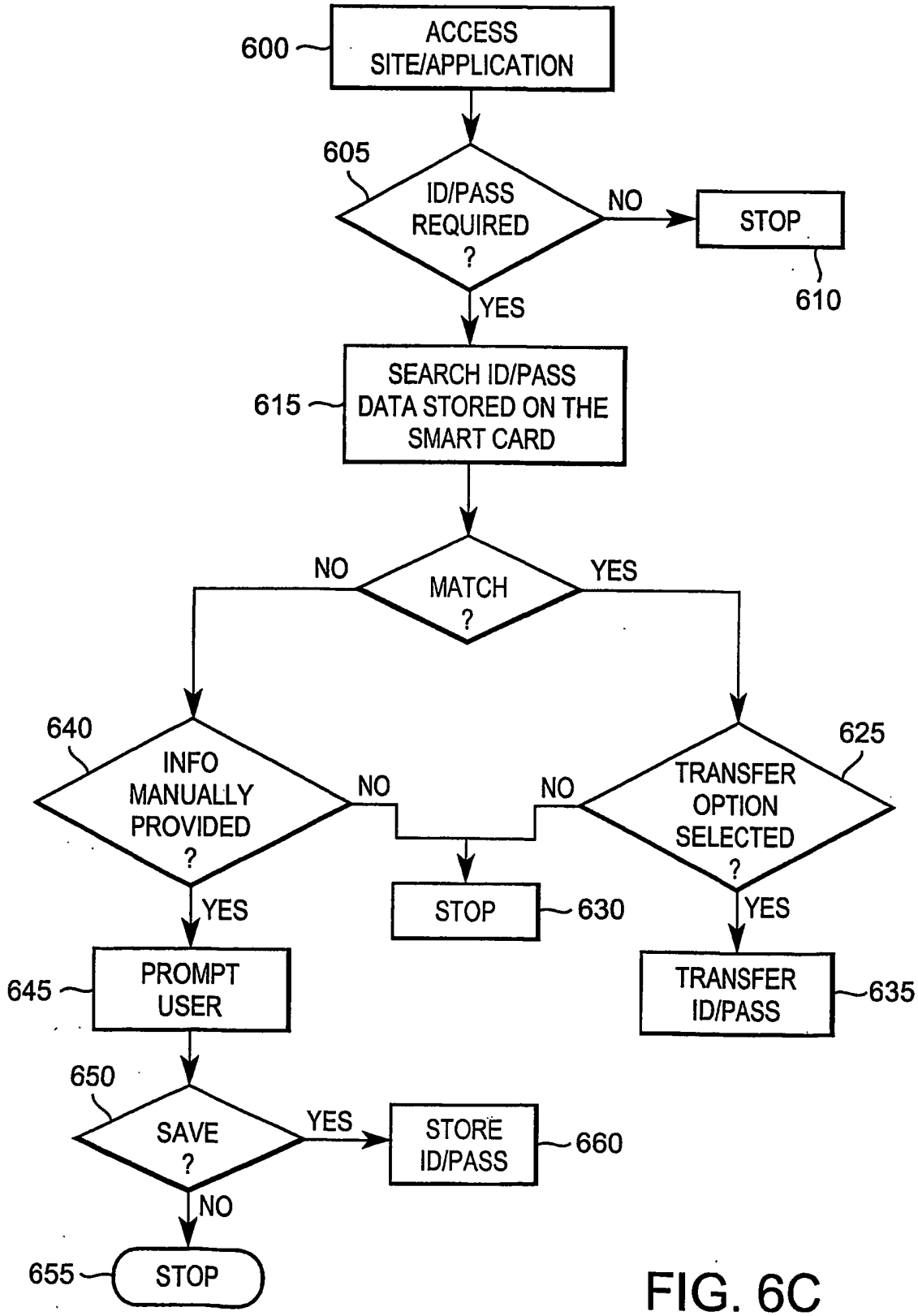

600
ACCESS SITE/APPLICATION
605
ID/PASS REQUIRED ?
NO
STOP
610
YES
615
SEARCH ID/PASS DATA STORED ON THE SMART CARD
NO
MATCH ?
YES
640
INFO MANUALLY PROVIDED ?
NO
NO
625
TRANSFER OPTION SELECTED ?
YES
STOP
630
YES
645
PROMPT USER
TRANSFER ID/PASS
635
650
SAVE ?
YES
STORE ID/PASS
660
NO
655
STOP

FIG. 6C

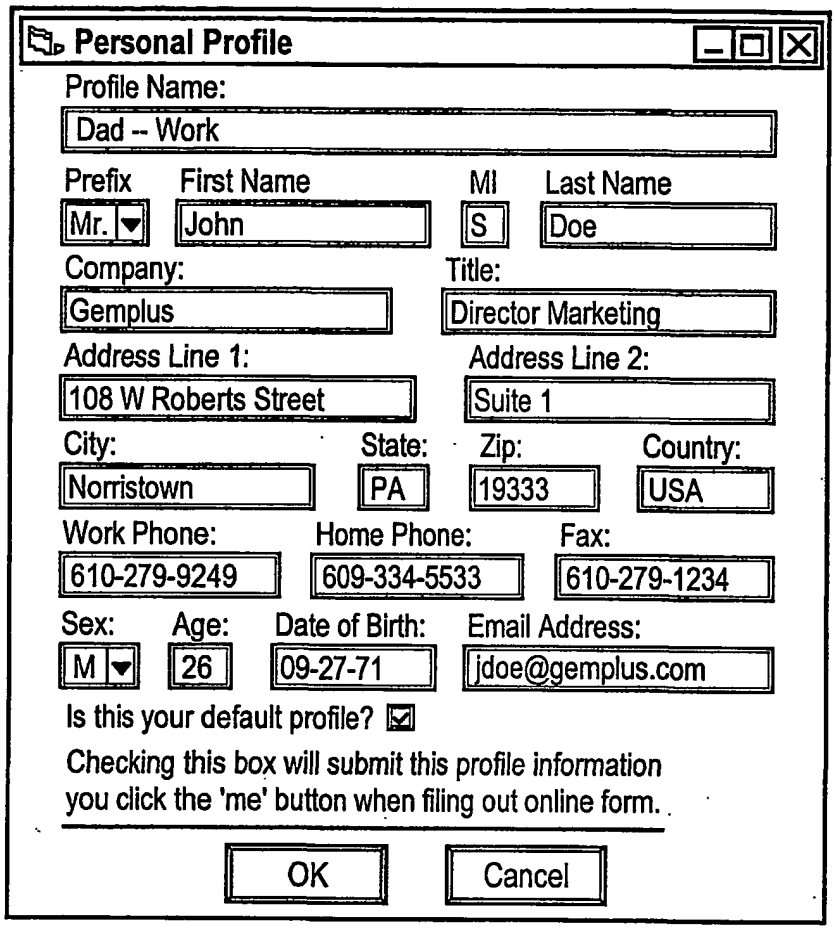

Personal Profile
Profile Name:
Dad -- Work
Prefix
First Name
MI
Last Name
Mr.
John
S
Doe
Company:
Title:
Gemplus
Director Marketing
Address Line 1:
Address Line 2:
108 W Roberts Street
Suite 1
City:
State:
Zip:
Country:
Norristown
PA
19333
USA
Work Phone:
Home Phone:
Fax:
610-279-9249
609-334-5533
610-279-1234
Sex:
Age:
Date of Birth:
Email Address:
M
26
09-27-71
jdoe@gemplus.com
Is this your default profile?
Checking this box will submit this profile information
you click the 'me' button when filing out online form.
OK
Cancel

FIG. 7A

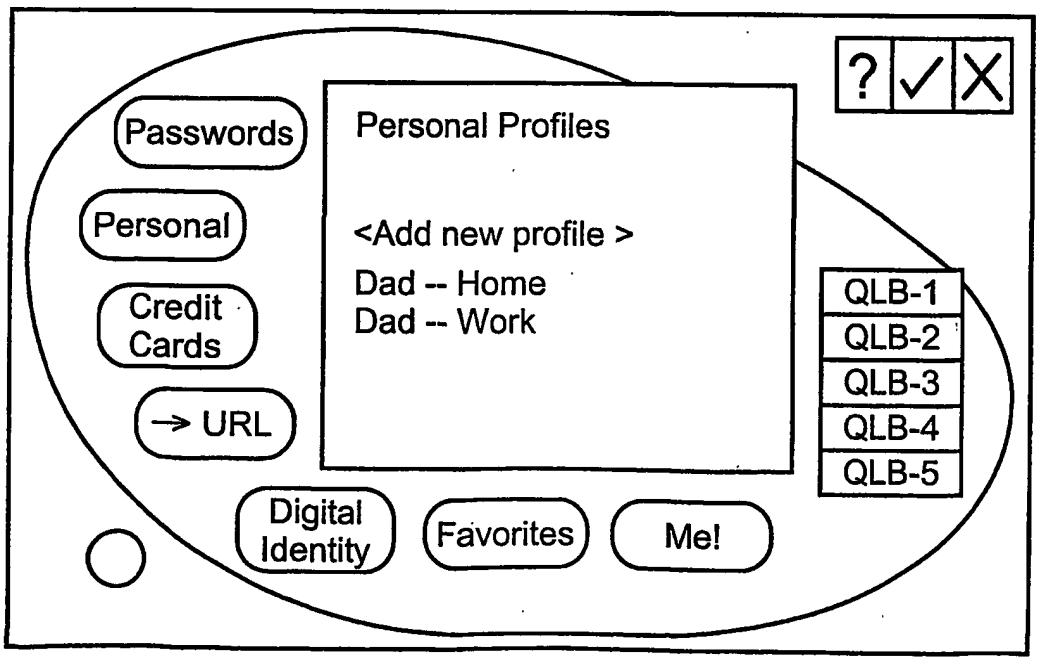

Passwords
Personal
Credit Cards
→ URL
Personal Profiles
<Add new profile >
Dad -- Home
Dad -- Work
QLB-1
QLB-2
QLB-3
QLB-4
QLB-5
Digital Identity
Favorites
Me!

FIG. 7B

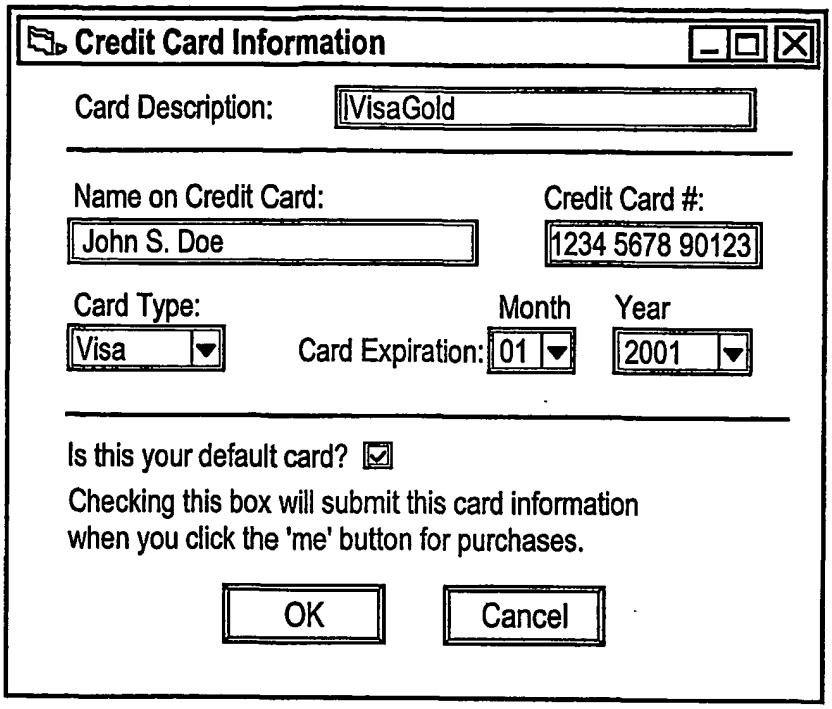

Credit Card Information
Card Description:
VisaGold
Name on Credit Card:
John S. Doe
Credit Card #:
1234 5678 90123
Card Type:
Visa
Card Expiration:
Month
01
Year
2001
Is this your default card?
Checking this box will submit this card information when you click the 'me' button for purchases.
OK
Cancel

FIG. 8A

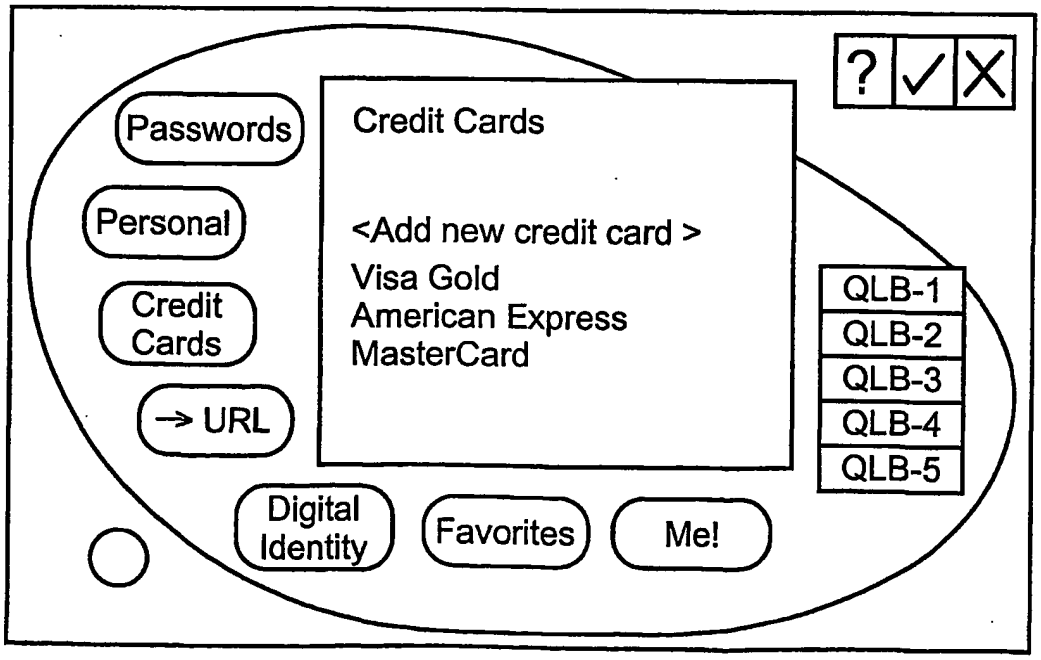

Passwords
Personal
Credit Cards
→ URL
Credit Cards
<Add new credit card >
Visa Gold
American Express
MasterCard
QLB-1
QLB-2
QLB-3
QLB-4
QLB-5
Digital Identity
Favorites
Me!

FIG. 8B

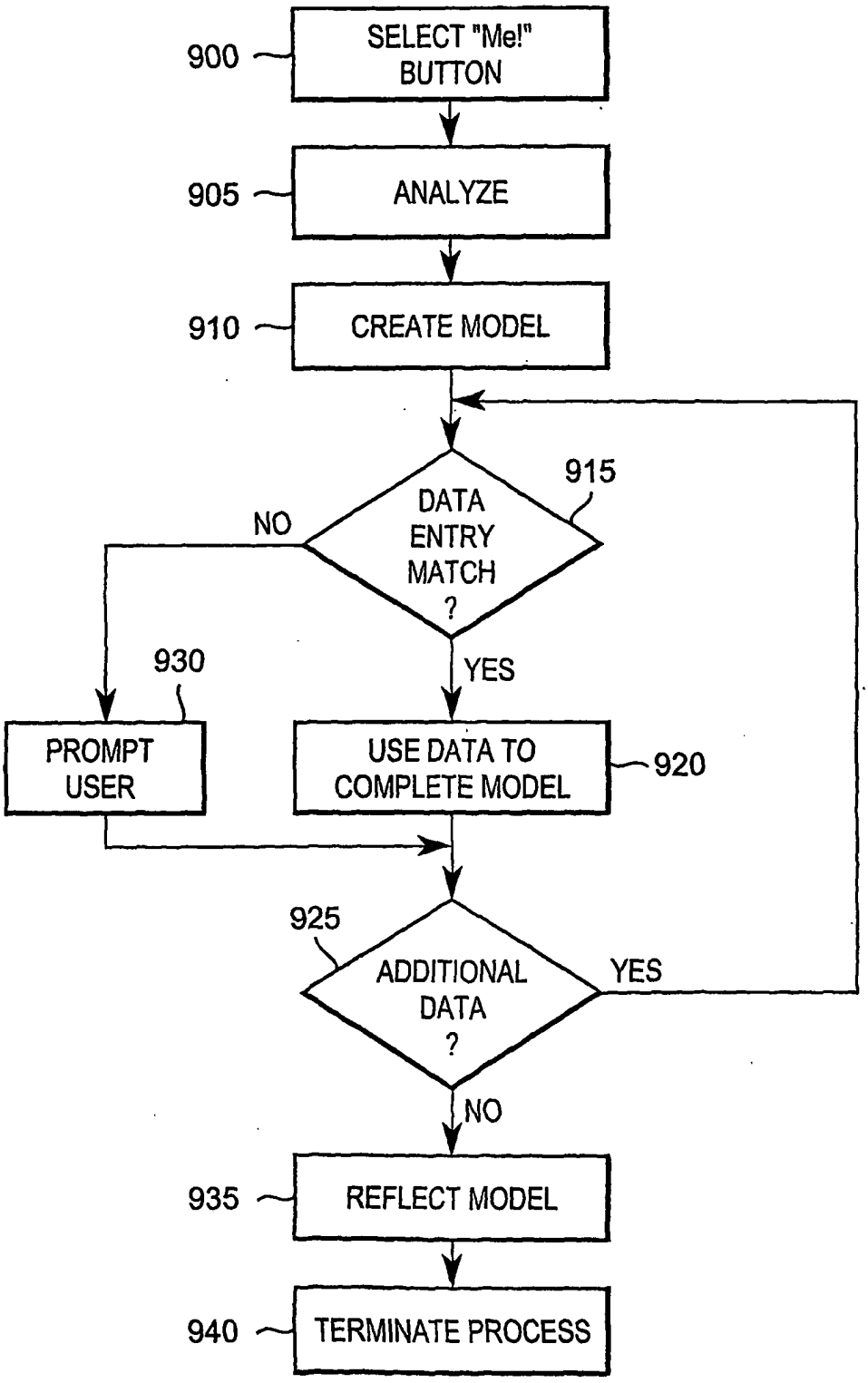

900
SELECT "Me!" BUTTON
905
ANALYZE
910
CREATE MODEL
915
DATA ENTRY MATCH ?
NO
YES
930
PROMPT USER
USE DATA TO COMPLETE MODEL
920
925
ADDITIONAL DATA ?
YES
NO
935
REFLECT MODEL
940
TERMINATE PROCESS

FIG. 9

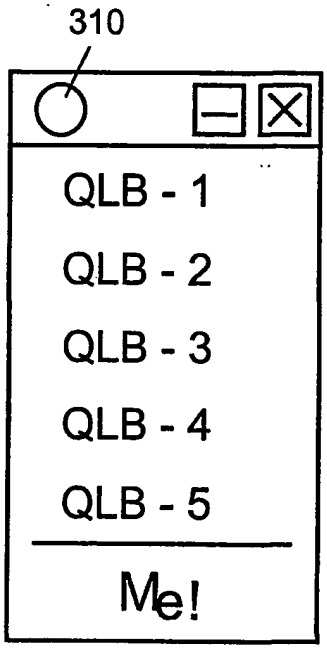


FIG. 10A

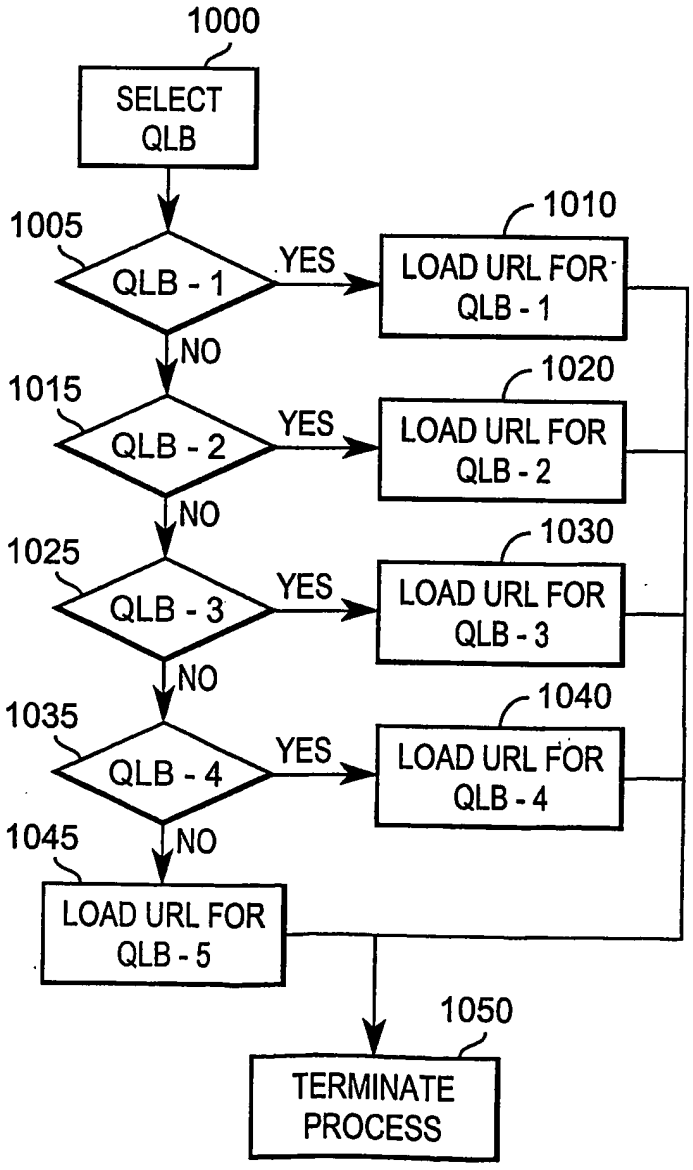


FIG. 10B

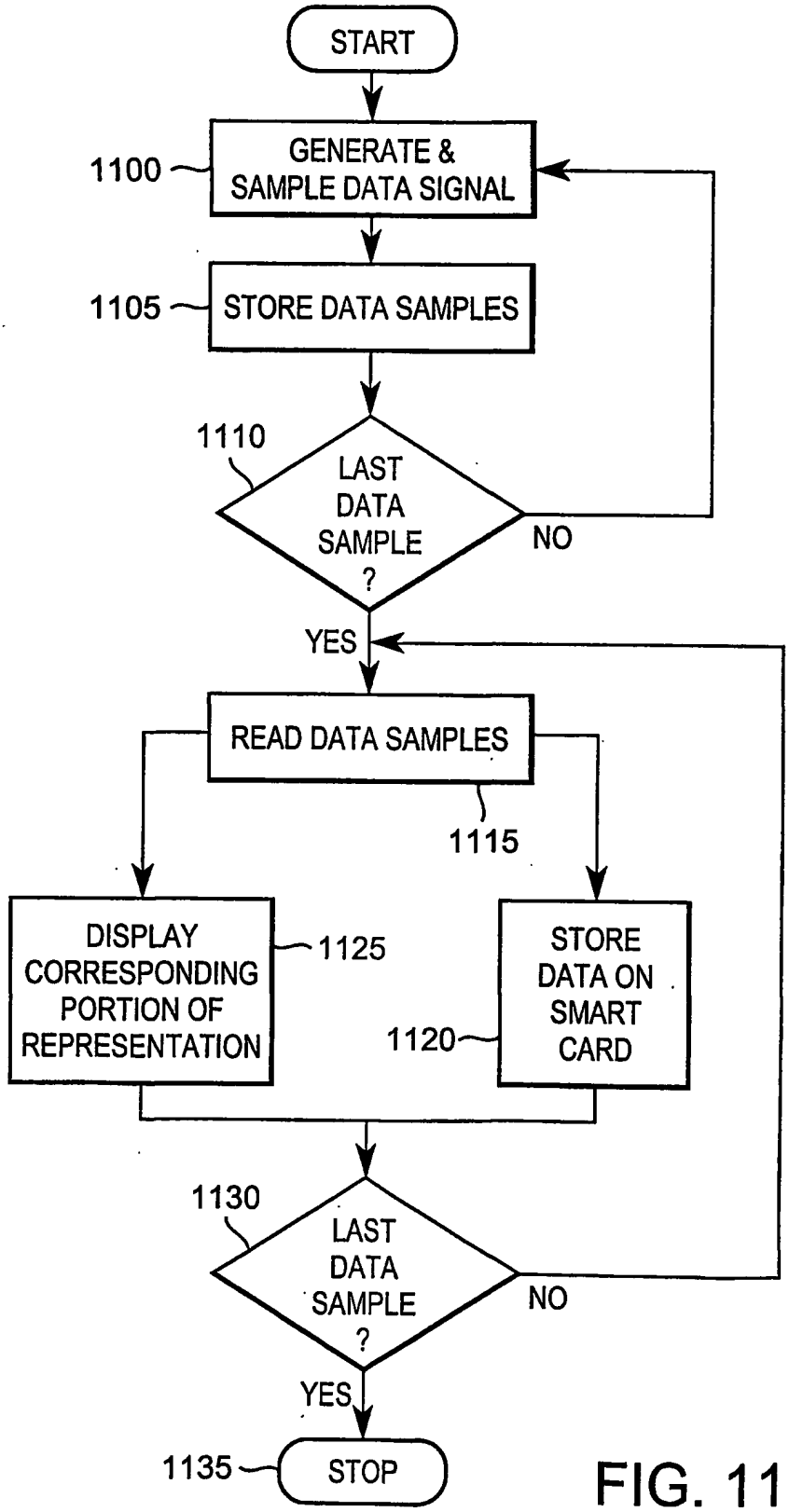

START
GENERATE & SAMPLE DATA SIGNAL
1100
STORE DATA SAMPLES
1105
1110
LAST DATA SAMPLE ?
NO
YES
READ DATA SAMPLES
1115
DISPLAY CORRESPONDING PORTION OF REPRESENTATION
1125
STORE DATA ON SMART CARD
1120
1130
LAST DATA SAMPLE ?
NO
YES
1135
STOP

FIG. 11

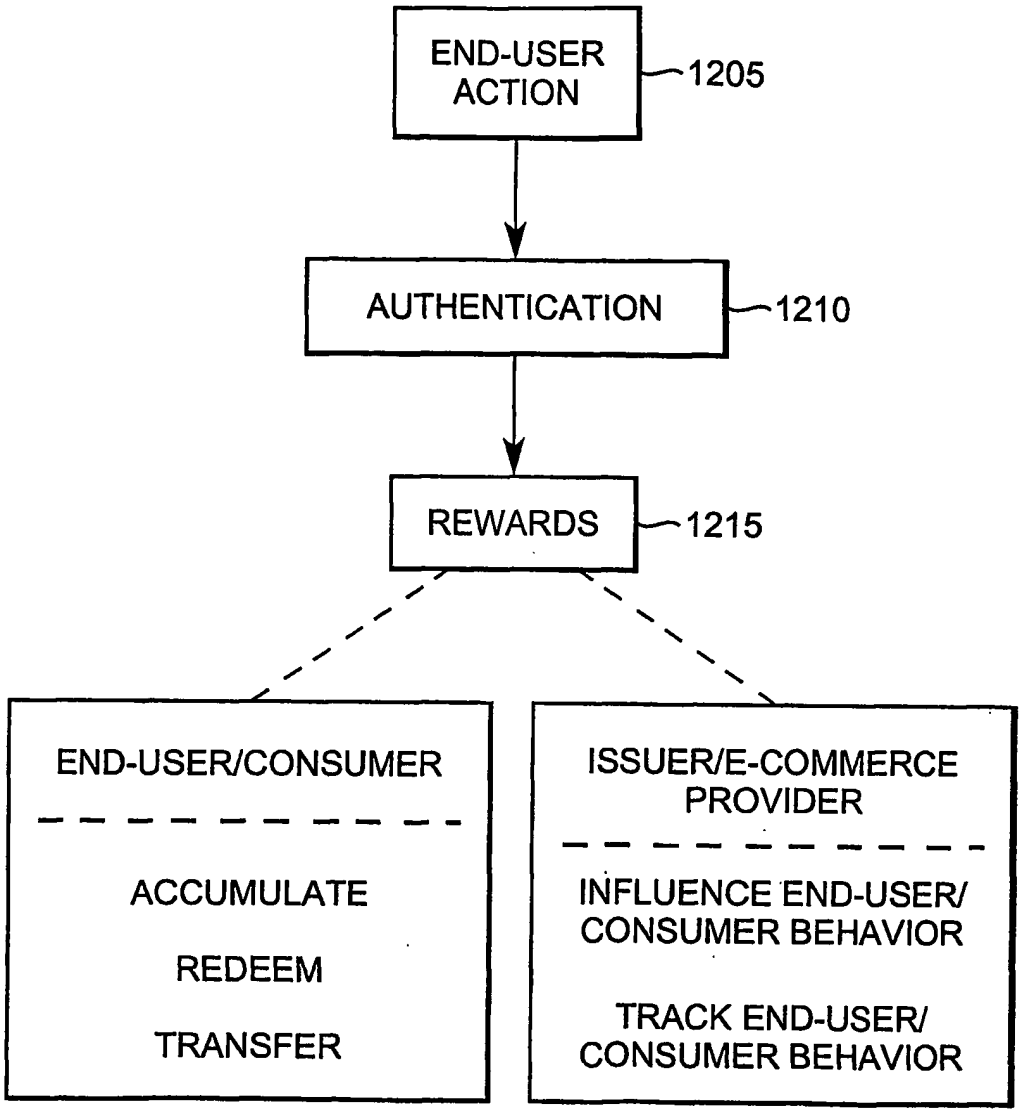

END-USER ACTION
1205
AUTHENTICATION
1210
REWARDS
1215
END-USER/CONSUMER
ACCUMULATE
REDEEM
TRANSFER
ISSUER/E-COMMERCE PROVIDER
INFLUENCE END-USER/ CONSUMER BEHAVIOR
TRACK END-USER/ CONSUMER BEHAVIOR

FIG. 12

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US01/28538

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) :G06F 15/173, 15/16

US CL : 709/226, 229; 713/172; 380/24; 379/144

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 709/226, 229; 713/172; 380/24; 379/144

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

Please See Extra Sheet.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y,P	US 6,199,114 B1 (WHITE et al) 06 March 2001, abstract, figures 1, 3, 6, 7, 8, col. 1 lines 61-col. 2 lines 1-22, col. 3 lines 56-col. 4 lines 1-67, col. 5 lines 10-32, col. 7 lines 9-30, col. 10 lines 36-64.	1-59
Y,P	US 6,173,400 B1 (PERLMAN et al) 09 January 2001, abstract, figures 1, 9, col. 2 lines 12-27, col. 5 lines 19-64, col. 12 lines 1-41.	1-59
Y	US 5,710,887 A (CHELLIAH et al) 20 January 1998, abstract, figures 1, 2, 5, 8, 12, col. 2 lines 4-34, col. 3 lines 47-col. 4 lines 1-48, col. 10 lines 14-55, col. 14 lines 40-59, col. 16 lines 3-67, col. 28 lines 52-col. 29 lines 23.	1-59

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26 OCTOBER 2001	06 NOV 2001
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer AYAZ R. SHEIKH Telephone No. (703) 305-9648

Form PCT/ISA/210 (second sheet) (July 1998)*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US01/28538

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 6,058,373 A (BLINN et al) 02 May 2000, abstract, figures 1, 2, col. 2 lines 4-67, col. 3 lines 1-col. 4 lines 14, col. 13 lines 35-col. 14 lines 25.	1-59
A, P	US 6,122,355 A (STROHL) 19 September 2000, abstract, figures 1, 2, 4, col. 1 lines 19-51.	1-59
A	US 5,604,802 A (HOLLOWAY) 18 February 1997, abstract, figures 2, 3, col. 1 lines 57-col. 2 lines 55.	1-59

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US01/28538

B. FIELDS SEARCHED
Electronic data bases consulted (Name of data base and where practicable terms used):

EAST, WEST
search terms: smart card, intergrated circuit card, chip card, memory card, samrt device, peripheral device, GUI, remote network server, order on-line, buy on-line, network devices, network connection and network operation, display and re-display on-line form.